Kapitel 2: VLANs

Kapitelaufbau

2.1 Segmentierung mit VLANs

2.2 Implementation von VLANs

2.3 Inter-VLAN Routing

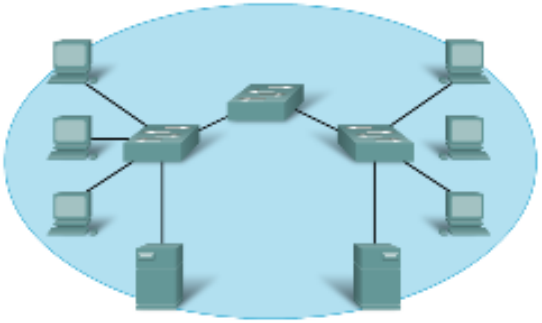
Kapitel 2: VLANs

Lernziele:

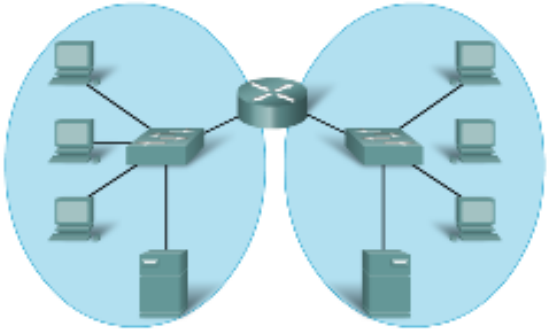
- Sie können erklären, weshalb und wozu man VLANs macht
- Sie verstehen, wie ein Switch Rahmen von verschiedenen VLANs weiterleitet
- Sie verstehen den Unterschied zwischen Access- und Trunk-Ports
- Sie können VLANs, Trunkports und Accessports konfigurieren
- Sie können Fehler in der VLAN-Konfiguration finden und beheben
- Sie verstehen die verschiedenen Ansätze, VLANs über einen Router miteinander zu verbinden.
- Sie verstehen, was man machen muss, damit ein Router mit dem VLAN-Tagging der Rahmen umgehen kann.
- Sie können Inter-VLAN Routing richtig konfigurieren.

2.1 Segmentierung mit VLANs

Reines Switching

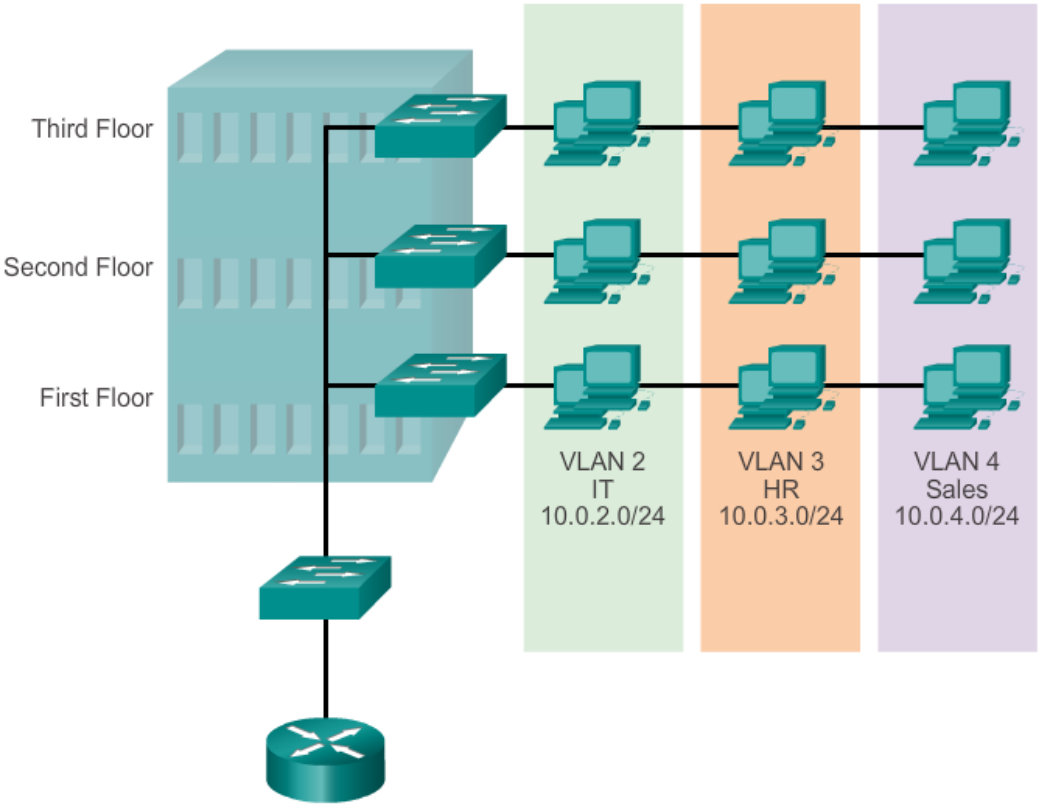


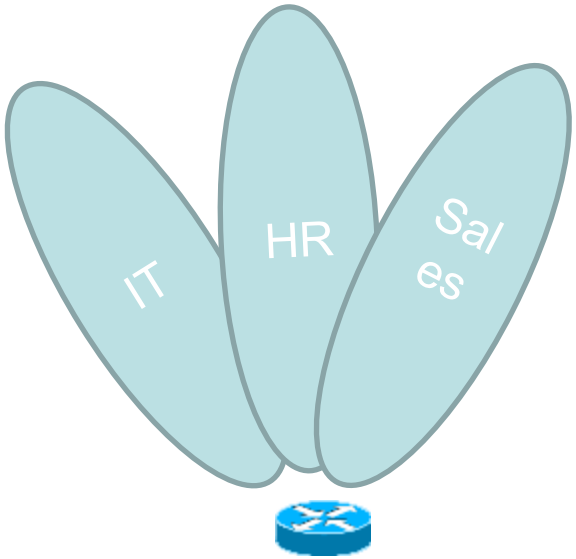
Routing



	Vorteile	Nachteile
Reines Switching		
Routing		

2.1 Segmentierung mit VLANs





2.1 Segmentierung mit VLANs

Eine Benutzergruppe	Mehrere Benutzergruppen
-Ein IP-Netz	-Mehrere IP-Netze
-Ein LAN	-Mehrere VLANs

Vorteile von VLANs:

- Weniger Broadcastverkehr
- Mehr Sicherheit
- Bessere Ausnutzung der Infrastruktur

2.1 Segmentierung mit VLANs

Typen von VLANs

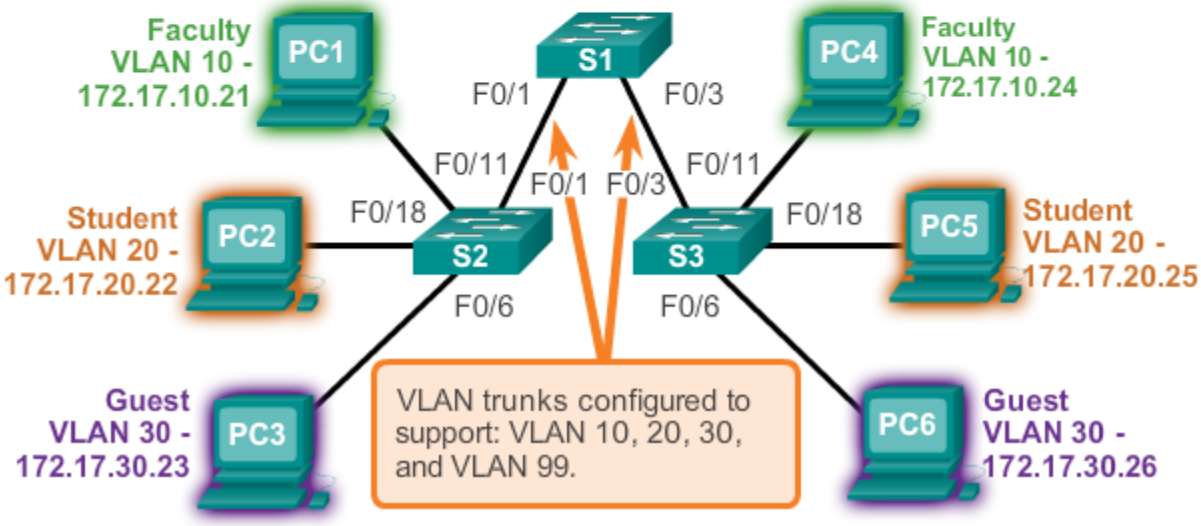
- Daten-VLANs für Benutzergruppen
- Default-VLAN: VLAN 1. Dieses VLAN kann nicht gelöscht werden. L2 Control Traffic wie STP (Spanning Tree Protocol), DTP (Dynamic Trunking Protocol) und CDP (Cisco Discovery Protocol) laufen über VLAN 1.
- Mgmt VLAN für die Administratoren und die Netzelemente
- Blackhole VLAN
- Voice VLAN
- Native VLAN (aus Rückwärts-Kompatibilitätsgründen)

2.1 Segmentierung mit VLANs

Beispiel-Topologie

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 Management and Native - 172.17.99.0/24

F0/1-5 are 802.1Q trunk interfaces with native VLAN 99.
F0/11-17 are in VLAN 10.
F0/18-24 are in VLAN 20.
F0/6-10 are in VLAN 30.



2.1 Segmentierung mit VLANs

Unterscheidung

- Access Ports (Fa0/6, 11 und 18): Anschluss von Endgeräten. Ein Rahmen, der von einem Endgerät kommt und in einen Switch eintritt, erhält einen „Tag“ mit der VLAN-ID in den Ethernet-Header. Ein Access-Port ist einem VLAN zugeordnet.
- Trunk Ports (Fa0/1 und 3): Verbindungen von Switch zu Switch. Die Ethernet-Rahmen haben einen Tag, der angibt, zu welchem VLAN sie gehören.

2.1 Segmentierung mit VLANs

Default Status eines Switch

```
Switch#show vlan brief
VLAN Name Status Ports
---- ---------- -------- ------------------------------
1    default    active   Fa0/1, Fa0/2, Fa0/3, Fa0/4
                         Fa0/5, Fa0/6, Fa0/7, Fa0/8
                         Fa0/9, Fa0/10, Fa0/11, Fa0/12
                         Fa0/13, Fa0/14, Fa0/15,Fa0/16
                         Fa0/17, Fa0/18, Fa0/19, Fa0/20
                         Fa0/21, Fa0/22, Fa0/23, Fa0/24
                         Gig0/1, Gig0/2
1002 fddi-default active
1003 token-ring-default active
1004 fddinet-default active
1005 trnet-default active
```

2.1 Segmentierung mit VLANs

Definition des VLAN-Tag nach IEEE 802.1Q

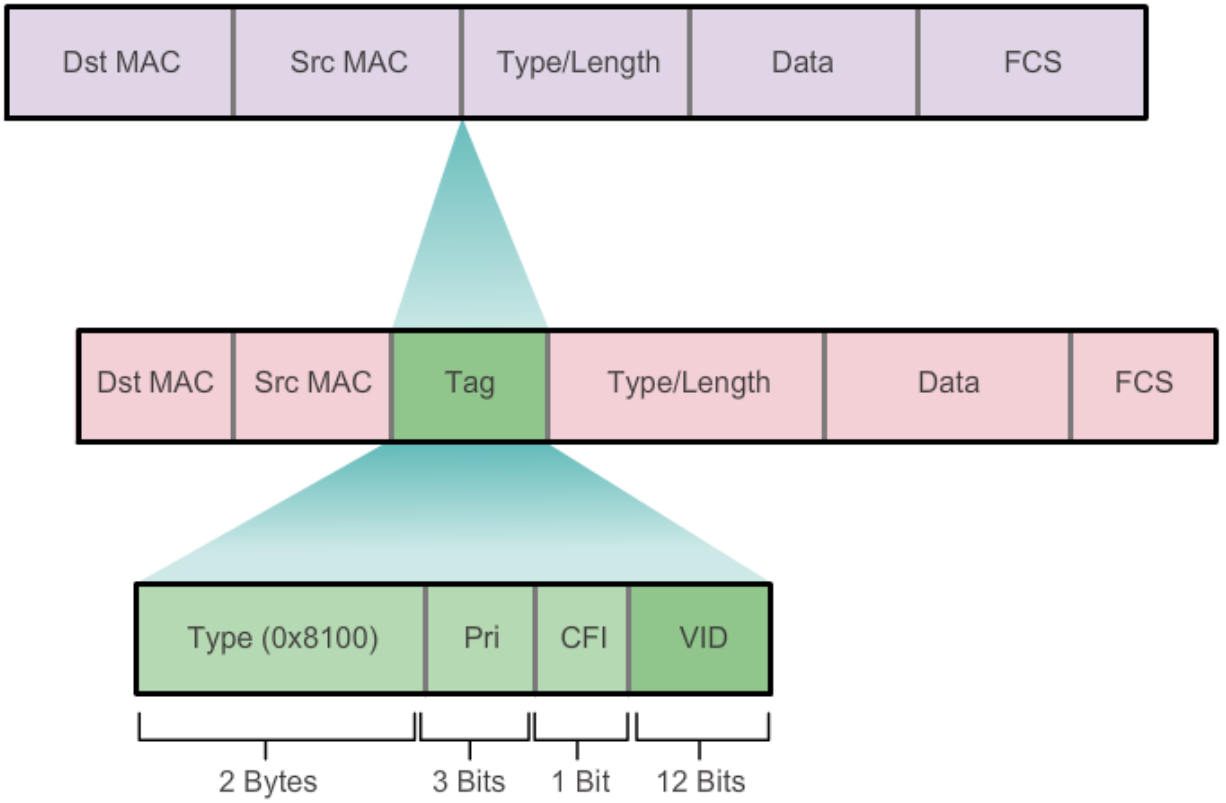
Pri: Priorität

CFI:

Canonical

Format

Indicator



2.1 Segmentierung mit VLANs

Kapselungsmethoden:

- Dot1q (IEEE 802.1Q)
- ISL (Inter Switch Link, ältere Version von Cisco)

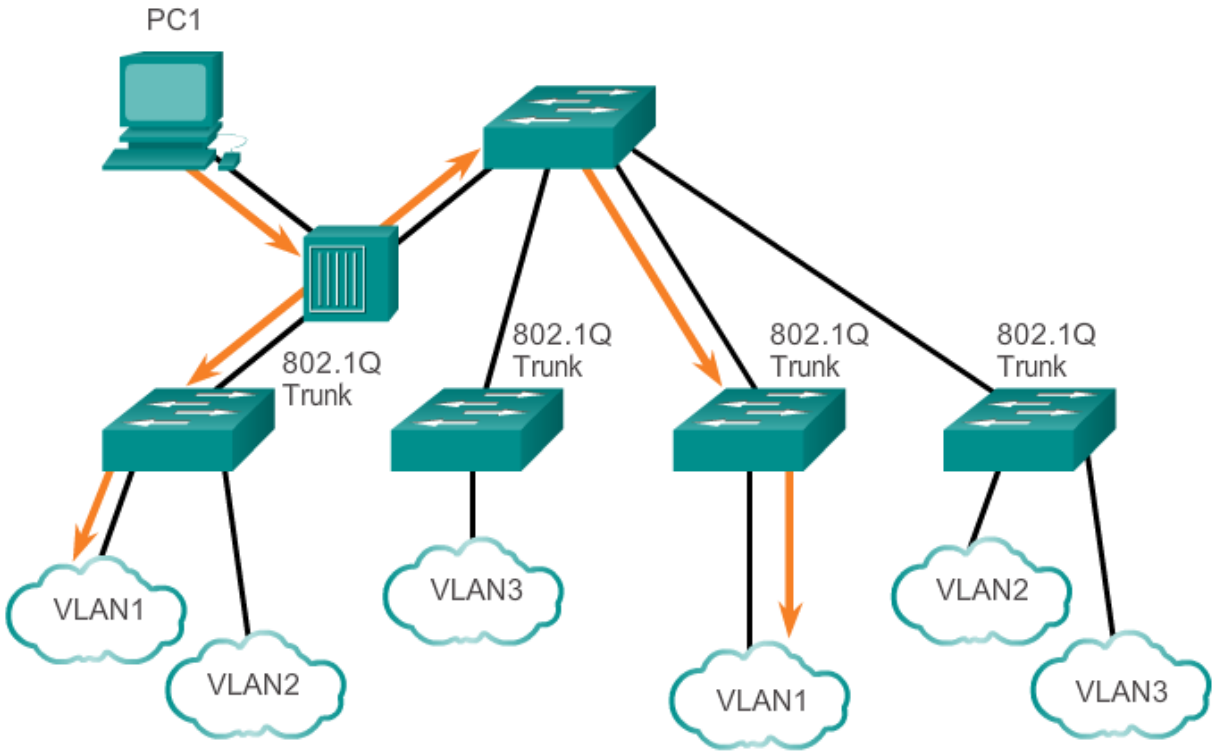
2960er Switch untrstützen nur dot1q. Grössere Cisco Switch unterstützen auch ISL. Hier ist eine Konfiguration notwendig, welche Kapselung gewählt werden soll.

Kompatibilität mit nicht VLAN-fähigen Geräten:

- Ältere oder billige Switch / Hub kennen den VLAN-Tag nicht.
- Für das «native VLAN» werden keine Tags gesetzt.
- Rahmen ohne VLAN Tag werden von VLAN-fähigen Switch dem native VLAN zugeordnet.
- Default: Das native VLAN hat die VLAN-ID 1.

2.1 Segmentierung mit VLANs

Anwendung des native VLAN: Der PC1 landet im native VLAN.



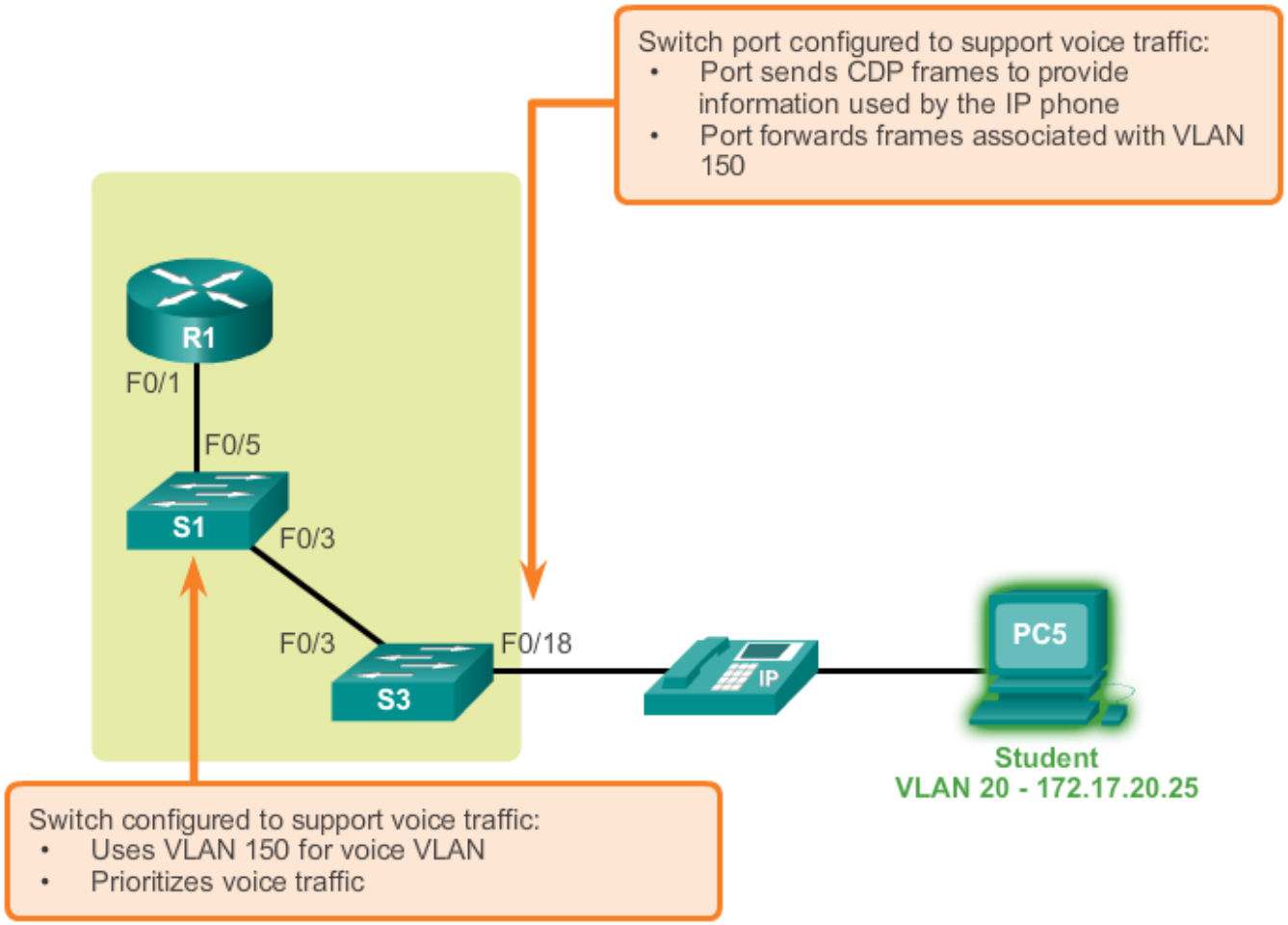
2.1 Segmentierung mit VLANs

VLANs und Switching-Tabelle:

- Für jedes VLAN gibt es eine logische MAC-Tabelle
- Jeder Rahmen in einem Switch hat ein VLAN-Tag und damit eine VLAN-ID *n*. Er wird der MAC-Tabelle *n* zugeführt und entsprechend dieser Tabelle weitergeleitet.
- Wird der Rahmen auf einen Access-Port weitergeleitet, so wird ihm beim Verlassen des Switch der VLAN-Tag entfernt.
- Wird der Rahmen auf einen Trunk-Port befördert, so behält er den VLAN-Tag.

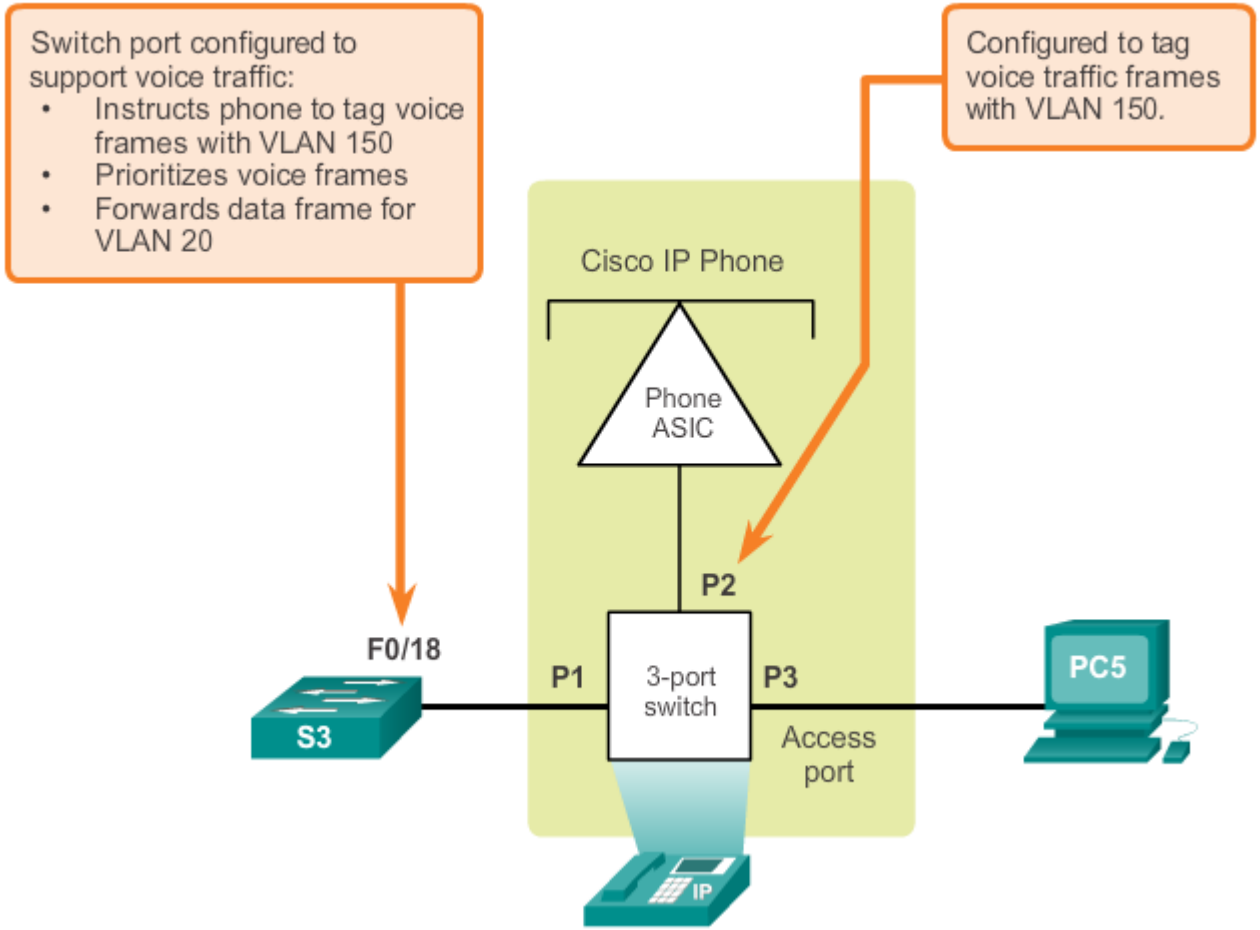
2.1 Segmentierung mit VLANs

Voice VLAN



2.1 Segmentierung mit VLANs

Voice VLAN



2.2 Implementation von VLANs

VLAN Nummerierung:

- “Normal range”: VLAN ID 1 bis 1005. VLAN 1 und die VLANs 1002 bis 1005 (Token Ring, FDDI) sind auf einem Cisco-Switch standardmässig vorhanden.
- “Extended range”: VLAN IDs von 1006 bis 4094. Die 802.1Q-Norm lässt 4000 VLANs zu (12 bit). Dies ist aber eher theoretischer Natur.

Praxis: Auf einem Cisco 2960-Switch können maximal 255 VLANs konfiguriert werden.

2.2 Implementation von VLANs

Wo werden diese VLANs gespeichert?

- Bei den 2900er-Switch, wird die VLAN-Information im Flash in der Datei vlan.dat und *nicht* in der Konfigurationsdatei running-config gespeichert.
- Bei den grösseren 4000/9000er-Switch kann es anders sein.
- Löschen unserer Access-Switch:

```
S1#erase startup-config
S1#delete flash:vlan.dat
```

- Werden VLANs konfiguriert, so muss man sie nach Beendigung eines Labors von Hand mit dem zweiten Befehl löschen. Auch wenn keine Konfiguration gespeichert wurde.

2.2 Implementation von VLANs

Erstellen eines VLANs:

```
S2(config)#vlan 10
S2(config-vlan)#name Verkauf
```

Ein Access-Port wird durch Konfiguration einem **VLAN zugewiesen**:

```
S2(config)#interface FastEthernet0/11
S2(config-if)#switchport mode access
S2(config-if)#switchport access vlan 10
```

Oder:

```
S2(config)#interface range FastEthernet0/11 - 17
S2(config-if)#switchport mode access
S2(config-if)#switchport access vlan 10
```

2.2 Implementation von VLANs

```
S2#show vlan brief
VLAN Name      Status    Ports
---- --------- --------- -------------------------------
1    default   active    Fa0/1, Fa0/2, Fa0/3, Fa0/4, Fa0/5,
                         Fa0/6, Fa0/7, Fa0/8, Fa0/9, Fa0/10
                         Fa0/18, Fa0/19, Fa0/20, Fa0/21
                         Fa0/22, Fa0/23, Fa0/24,
                         Gig0/1, Gig0/2
10   Verkauf  active    Fa0/11, Fa0/12, Fa0/13, Fa0/14,
                         Fa0/15, Fa0/16, Fa0/17
1002 fddi-default active
1003 token-ring-default active
1004 fddinet-default active
1005 trnet-default active
```

2.2 Implementation von VLANs

Konfiguration eines Trunk Ports auf C2960:

```
S2(config)#interface fa0/1
S2(config-if)#switchport mode trunk
```

Konfiguration eines Trunk Ports auf grösseren Switch (z.B. C3560):

```
S2(config-if)#switchport trunk encapsulation dot1q
S2(config-if)#switchport mode trunk
```

Auf Geräten, die IEEE802.1Q und ISL unterstützen, muss die Encapsulation festgelegt werden.

2.2 Implementation von VLANs

Kontrolle:

```
S2#show interface trunk
Port   Mode   Encapsulation Status Native vlan
Fa0/1  on     802.1q        trunking      1
Port   Vlans allowed on trunk
Fa0/1  1-1005
Port   Vlans allowed and active in management domain
Fa0/1  1,10
Port   Vlans in spanning tree forwarding state and not pruned
Fa0/1  1,10
```

2.2 Implementation von VLANs

Dynamic Trunking Protocol (DTP)

Welche Modi gibt es auf einem Switch-Port?

```
S1(config-if)#switchport mode ?
  access   Set trunking mode to ACCESS unconditionally
  dynamic  Set trunking mode to dynamically negotiate
                                      access or trunk mode
  trunk    Set trunking mode to TRUNK unconditionally
```

Für den Mode dynamic kommt das DTP zum Zug. Es gibt wiederum zwei Zustände für dynamic:

```
Switch(config-if)#switchport mode dynamic ?
  auto       Set trunking mode dynamic negotiation
             parameter to AUTO
  desirable  Set trunking mode dynamic negotiation
             parameter to DESIRABLE
```

2.2 Implementation von VLANs

Wahrheitstabelle für den Mode auf der Leitung

	Dynamic Auto	Dynamic Desirable	Trunk	Access
Dynamic Auto	Access	Trunk	Trunk	Access
Dynamic Desirable	Trunk	Trunk	Trunk	Access
Trunk	Trunk	Trunk	Trunk	-
Access	Access	Access	-	Access

2.2 Implementation von VLANs

In welchen Mode befindet sich eine Leitung?

```
S1#show interfaces switchport
Name: Fa0/1
Switchport: Enabled
Administrative Mode: dynamic auto
Operational Mode: trunk
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 99
```

2.2 Implementation von VLANs

Native VLAN: Per Default ist VLAN 1 das native VLAN

Änderung des native VLANs:

```
S1(config-if)#switchport trunk native vlan 99
S2(config-if)#switchport trunk native vlan 99
```

Einschränkung der VLANs, die über einen Trunk transportiert werden:

```
S1(config-if)#switchport trunk allowed vlan 10,99
```

2.2 Implementation von VLANs

Voice VLAN (Aufbau siehe Abschnitt 2.1)

```
S3(config)# vlan 20
S3(config-vlan)# name student
S3(config-vlan)# vlan 150
S3(config-vlan)# name VOICE
S3(config-vlan)# exit
S3(config)# interface fa0/18
S3(config-if)# switchport mode access
S3(config-if)# switchport access vlan 20
S3(config-if)# mls qos trust cos
S3(config-if)# switchport voice vlan 150
```

Die Konfiguration `mls qos trust cos` sorgt dafür, dass das Feld Priority im VLAN-Tag, wie vom Telefon gesetzt, unverändert hoch bleibt. Ohne die Konfiguration würde sie vom Switch zurück auf 0 gesetzt.

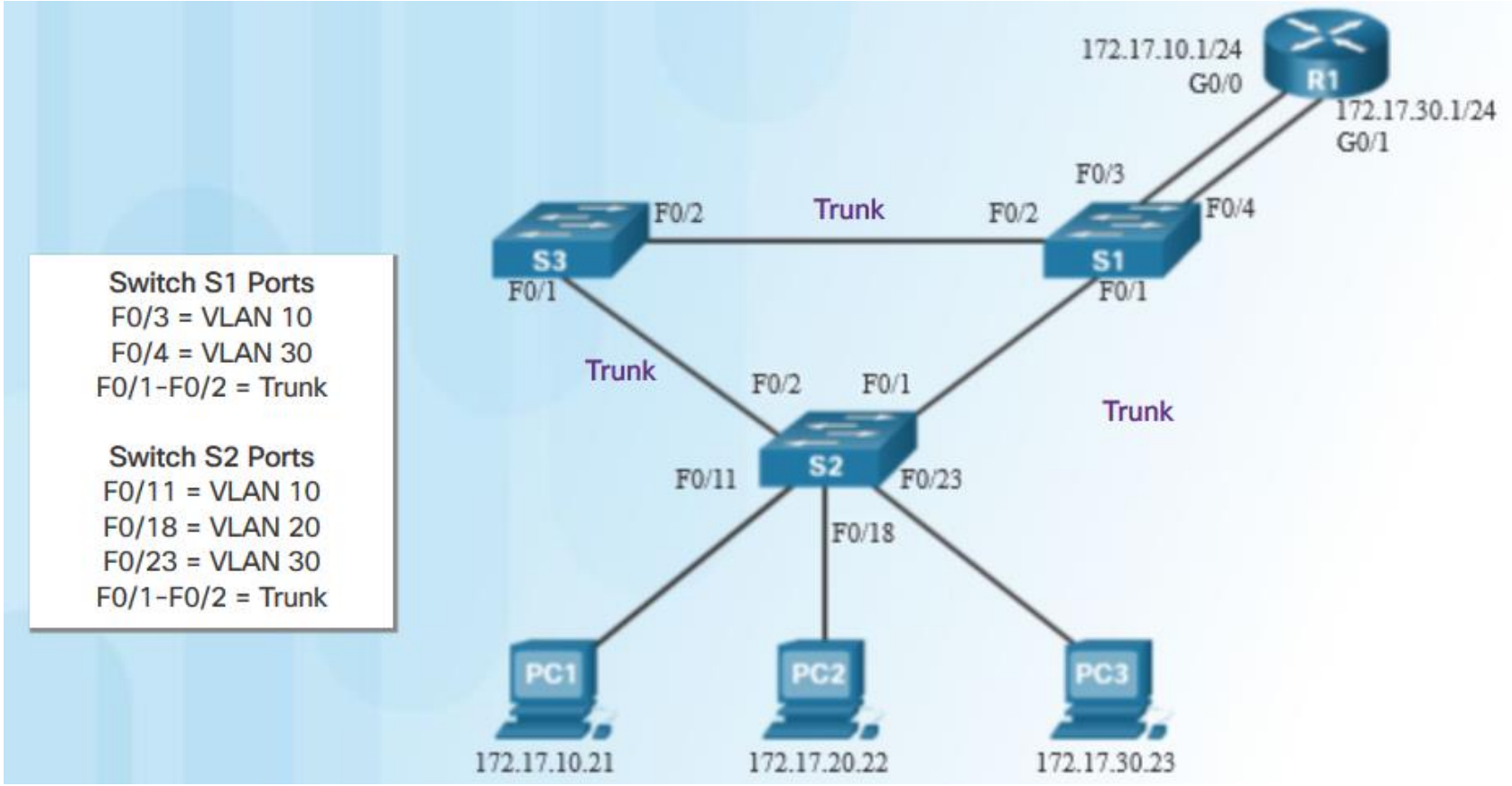
2.3 Inter-VLAN Routing

Beispiel Topologie aus dem ersten Abschnitt: Endgeräte aus Faculty VLAN können Endgeräte aus dem Student VLAN **nicht** erreichen. Vollständige Trennung.

Damit ein Endgerät aus seinem VLAN heraus kommunizieren kann, wird ein Router benötigt.

2.3 Inter-VLAN Routing

1. Ansatz: *Ein* VLAN pro Leitung zum Router

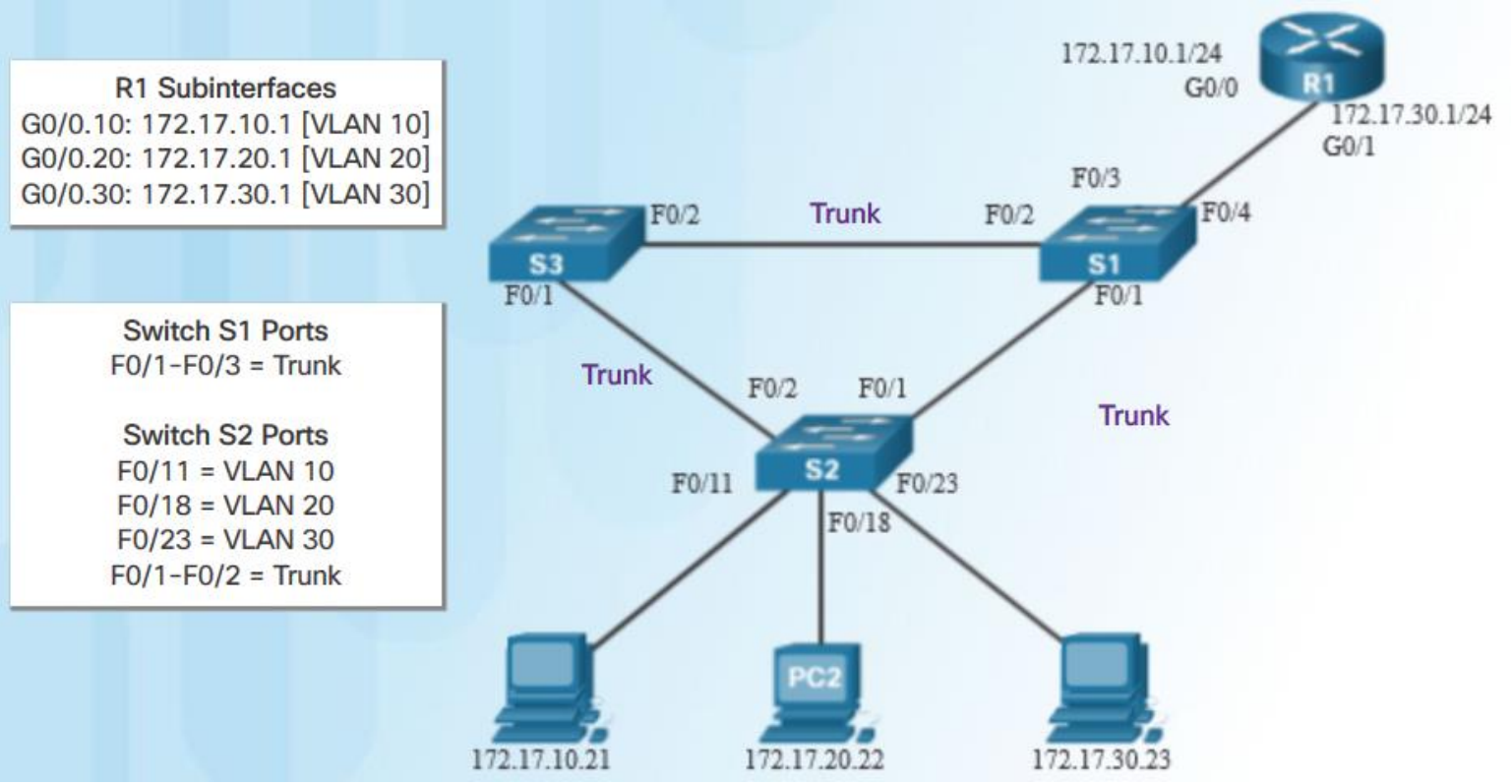


2.3 Inter-VLAN Routing

Switch kennen VLAN-Trunking mit IEEE 802.1Q. Gibt es etwas ähnliches für Router?

2.3 Inter-VLAN Routing

2. Ansatz: *Alle* VLANs gemultiplext über *eine* Trunk-Leitung zum Router führen.



2.3 Inter-VLAN Routing

Konfiguration auf dem Switch S1:

```
S1(config)#interface range Fa0/1, Fa0/2, Fa0/4
S1(config-if)#switchport mode trunk
```

Konfiguration Router:

Konfiguration von Sub-IFs auf dem phys. IF g0/0

```
R1(config)#interface G0/0
R1(config-if)#no ip address
R1(config-if)#no shutdown
R1(config)#interface g0/0.10
R1(config-if)#encapsulation dot1Q 10     //IF für VLAN 10
R1(config-if)#ip address 172.17.10.1 255.255.255.0
```

2.3 Inter-VLAN Routing

```
R1(config-if)#interface g0/0.20          //IF für VLAN 20
R1(config-if)#encapsulation dot1Q 20
R1(config-if)#ip address 172.17.20.1 255.255.255.0
R1(config-if)#interface g0/0.30          //IF für VLAN 30
R1(config-if)#encapsulation dot1Q 30
R1(config-if)#ip address 172.17.30.1 255.255.255.0
R1(config-if)#end
```

Ergebnis

Eingang: Rahmen mit IEEE-Tag und V-ID 10 werden dem logischen IF g0/0.10 zugeordnet.

Ausgang: Rahmen für das Netz 172.17.20.0 werden mit einem IEEE-Tag und VID 20 versehen und abgesendet.

2.3 Inter-VLAN Routing

Routing-Tabelle des Routers:

```
R1#show ip route
   172.17.0.0/16 is variably subnetted, 6 subnets, 2 masks
C      172.17.10.0/24 is directly connected, g0/0.10
L      172.17.10.1/32 is directly connected, g0/0.10
C      172.17.20.0/24 is directly connected, g0/0.20
L      172.17.20.1/32 is directly connected, g0/0.20
C      172.17.30.0/24 is directly connected, g0/0.30
L      172.17.30.1/32 is directly connected, g0/0.30
```