



Kommunikationstechnik KOTE / Netzwerkgrundlagen  
6. Unit

# Übersicht der einzelnen Modulblöcke (roter Faden)

**Grundlagen aus  
relevanten Kapiteln**  
Cisco CCNA 200-301  
Volume 1+2

**Modulaufgaben**  
Vorbereitung und  
Vertiefung

*Simulationsübungen  
mit dem CISCO  
Pakettracer und mit  
Wireshark*

**Stoffumfang KOTE:**

CCNA1/ Kap. 1 – 6 / 8 / 9 / 11 – 14 / 18

CCNA2/ Kap. 1 + 13

CCNA1/Kap. 2  
CCNA2/Kap. 13

**Grundlagen Netzwerkmanagement und  
Netzwerk**

NetAcad/Kap. 1

CCNA1/Kap. 1  
CCNA1/Kap. 3

**Netzwerkkommunikation LAN/WAN  
ISO/OSI Referenzmodell**

NetAcad/Kap. 3

CCNA2/Kap. 1

**Standards und Gremien  
L7,L4 und L3 analysieren**

NetAcad/Kap. 10  
NetAcad/Kap. 9

CCNA1/Kap. 11  
CCNA1/Kap. 12  
CCNA1/Kap. 13  
CCNA1/Kap. 14

**IPv4 Funktionen und Subnettierung**

NetAcad/Kap. 6  
NetAcad/Kap. 7  
NetAcad/Kap. 8

CCNA1/Kap. 4  
CCNA1/Kap. 5/6

**ICMP, Routing, Switching und CLI-Grundlagen**

NetAcad/Kap. 4  
NetAcad/Kap. 5

CCNA1/Kap. 8

**VLAN und IEEE 802.1Q konfigurieren**

CCNA1/Kap. 9

**Redundante Netzwerkdesigns**

CCNA1/Kap. 18  
(Commands)

**Netzwerk für ein KMU konfigurieren  
Troubleshooting im Netzwerk**

**NPDO - Netzwerk, Planung, Design und  
Optimierung**

**NIUS - Netzwerkinstallation und Störungsbehebung**

# Lernziele des 6. Modulblocks

- **Du kannst...**

1. ...die Grundlagen von VLANs (802.1Q) im Zusammenhang mit Netzwerkdesigns einordnen.
2. ...verschiedene Einsatzzwecke von VLANs erläutern.
3. ...einen Switch grundlegend konfigurieren.
4. ...VLANs auf Basis von 802.1Q selbstständig konfigurieren.

# Agenda

**«Repetition»**

# Gruppenarbeit

## Repetition Block 5

**Auftrag:** Jede Gruppe bereitet eines der folgenden 4 Themen soweit vor, dass sie es den Kollegen im Anschluss erklären kann.

**Form:** keine Vorgabe

**Zeit:** Vorbereitung 25 Minuten

**Themen:**

1. Wie merkt (lernt) sich ein Switch die Mac-Adressen?
2. Was ist der Sinn des ARP-Prozesses und wie läuft dieser ab?
3. Wichtige Funktionen eines Switches inkl. CLI-Modi
4. Wie funktioniert das Routing?

**Zeit: 25 Minuten**

# Fragen zu Kapitel 4 und 5

Besprechung der Fragen zu Kapitel 4 (Seite 85)  
zu zweit

- Zweiergruppe: Besprechung aller Fragen

**Zeit: 15 Minuten**

# Agenda



## «Grundlagen VLAN»

CCNA1 Kapitel 8

# IEEE 802.1Q

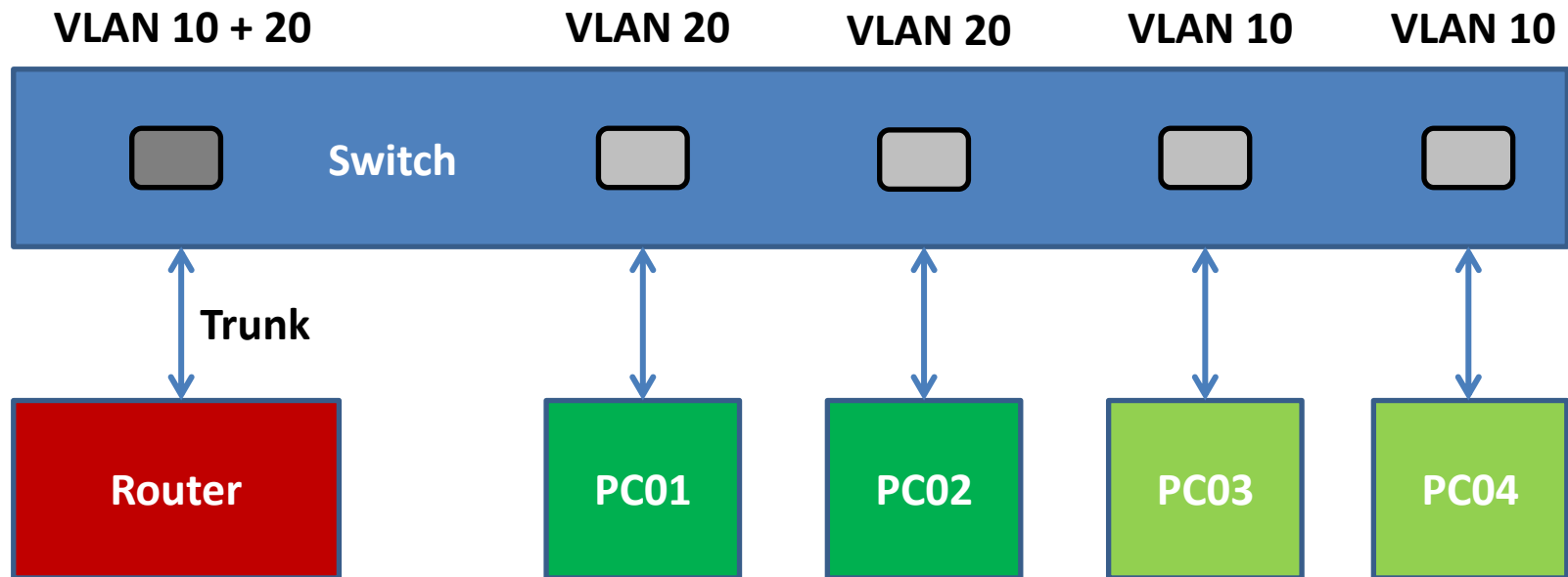
## VLAN Grundlagen

- VLANs sind logische Netzwerke innerhalb eines physischen Netzwerks
- Switches müssen dazu 802.1Q unterstützen (tagged VLAN)
- Üblicherweise weist der Switch auf dem Port ein VLAN-Tag hinzu.
- Ports können dabei zu mehreren VLANs gehören .
- Verbindungen zwischen Switches werden Trunk genannt (dort existieren Tags).
- VLANs sind eine Layer2 Technologie.
- Jedes VLAN hat ein eigenes IP-Subnetz. Daher ist ein VLAN eine eigene Broadcast-Domain.
- VLANs müssen durch Routing (z.B. L3-Switches) verbunden werden.



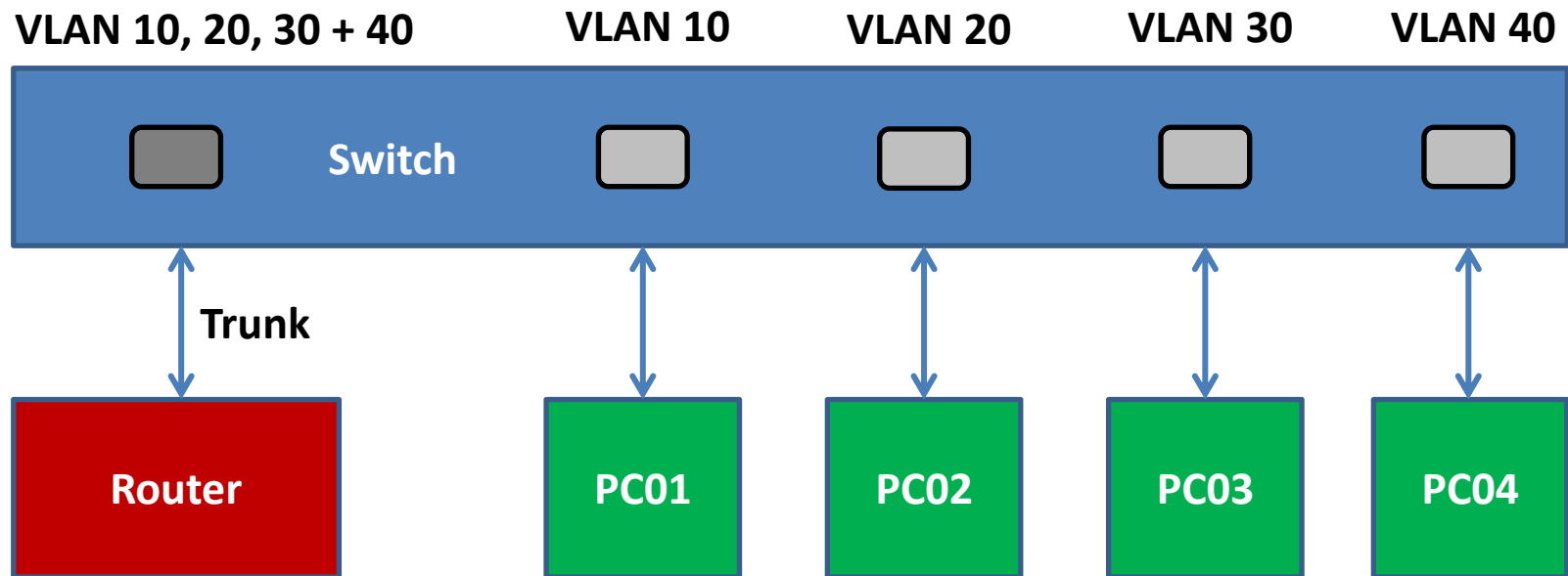
# VLAN Grundlagen 802.1Q (tagged)

- Ein Computer in einem VLAN 1 kann nicht mit einem Computer in einem VLAN 2 kommunizieren. Über den Router können die VLANs verbunden werden.



# VLAN Security 802.1Q (tagged)

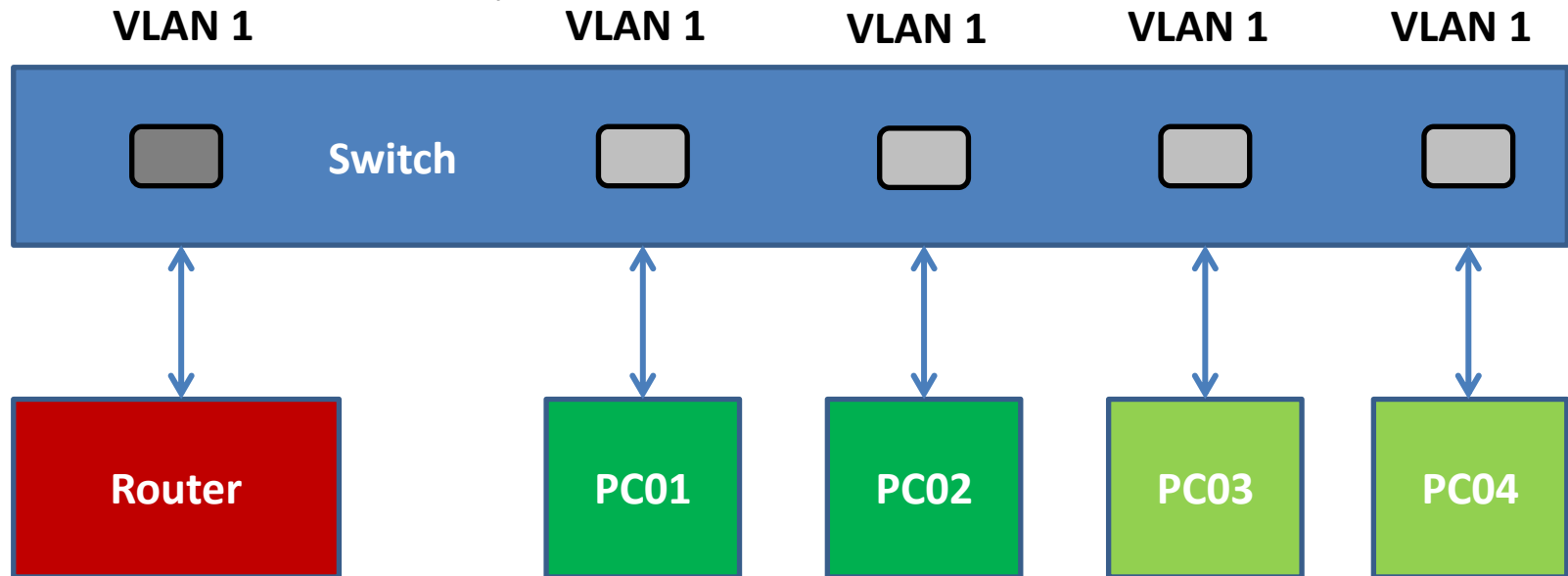
- Alle Computer sind in einem eigenen VLAN von allen anderen Computern getrennt.



# VLAN Grundlagen

## Natives/Default VLAN (Cisco **VLAN 1**)

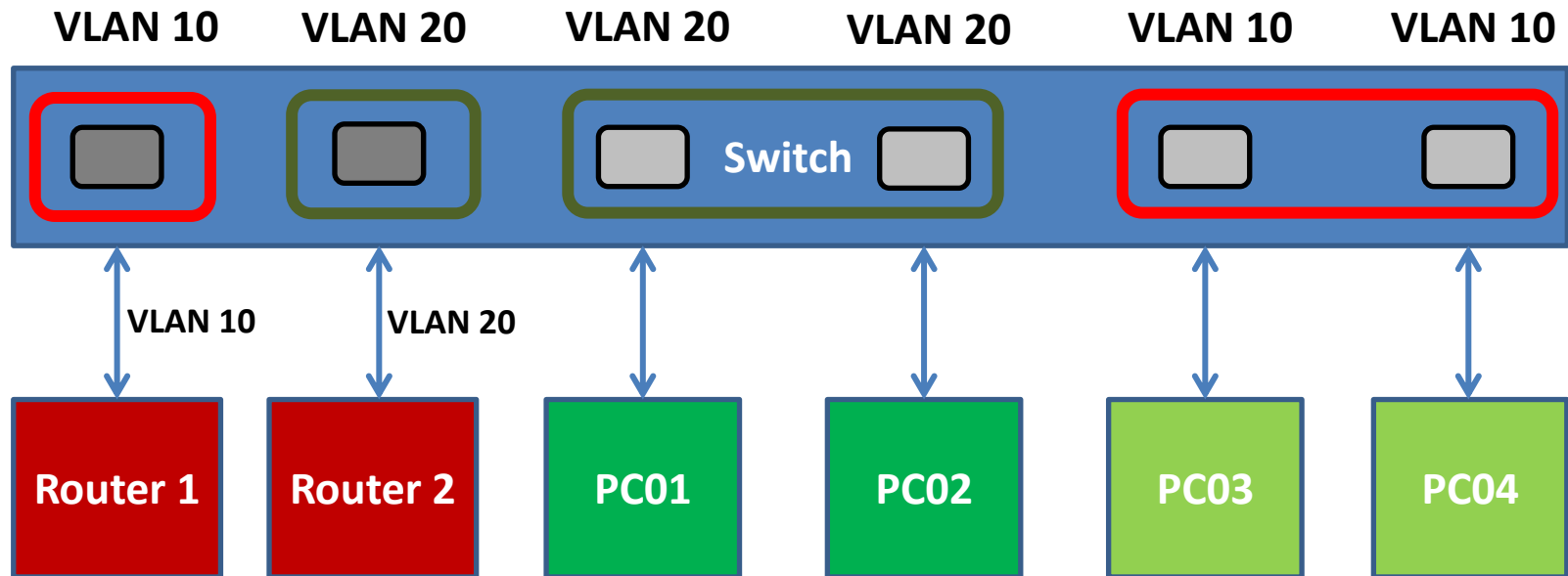
- **Nativ werden alle Port in das VLAN1 genommen** (Natives VLAN oder **Default VLAN**). VLAN1 erstellt kein VLAN-Tag und ermöglicht damit Kompatibilität zu nicht VLAN fähigen Netzgeräten. Das native (default) VLAN kann konfiguriert werden sollte aber auf allen Netzgeräten (Switch, Router, Access Point,..) das selbe sein!



# VLAN Grundlagen

## Portbasierte VLAN (Access Interfaces)

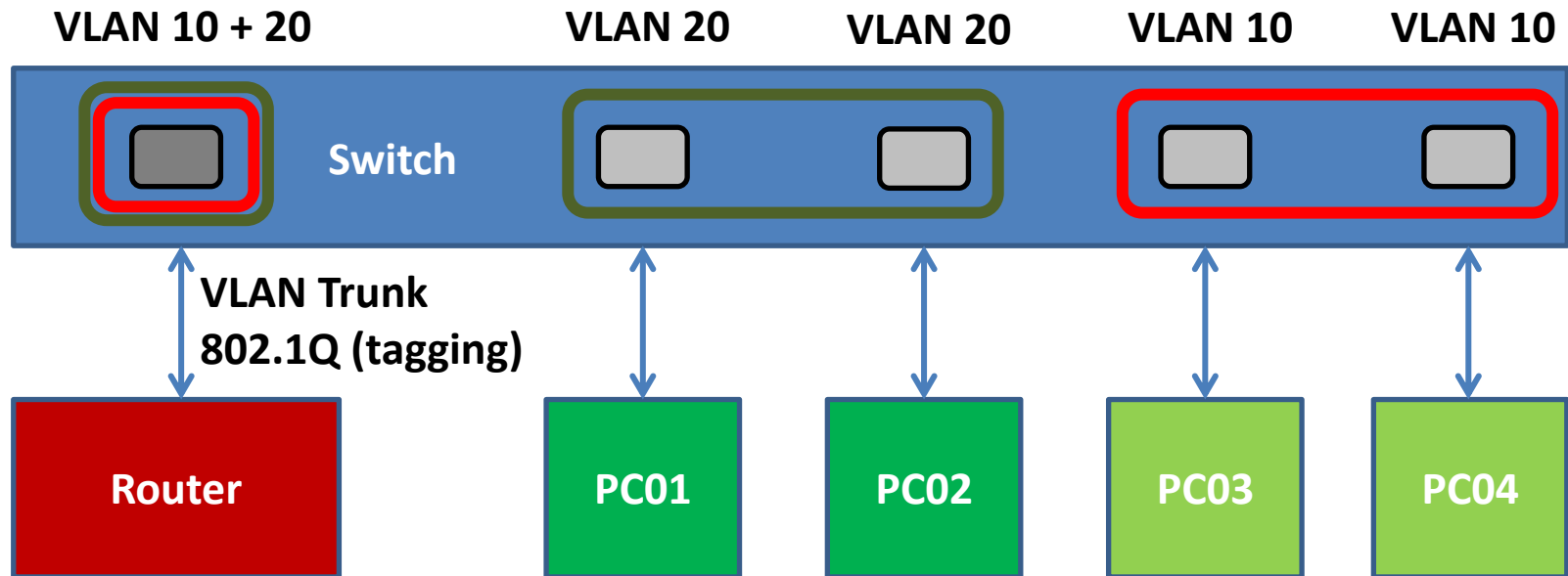
- Ein Computer in einem VLAN 10 kann nicht mit einem Computer in einem VLAN 20 kommunizieren. Bei **portbasierten VLANs** kann ein Interface nur einem VLAN angehören.



# VLAN Grundlagen

## 802.1Q (tagged)

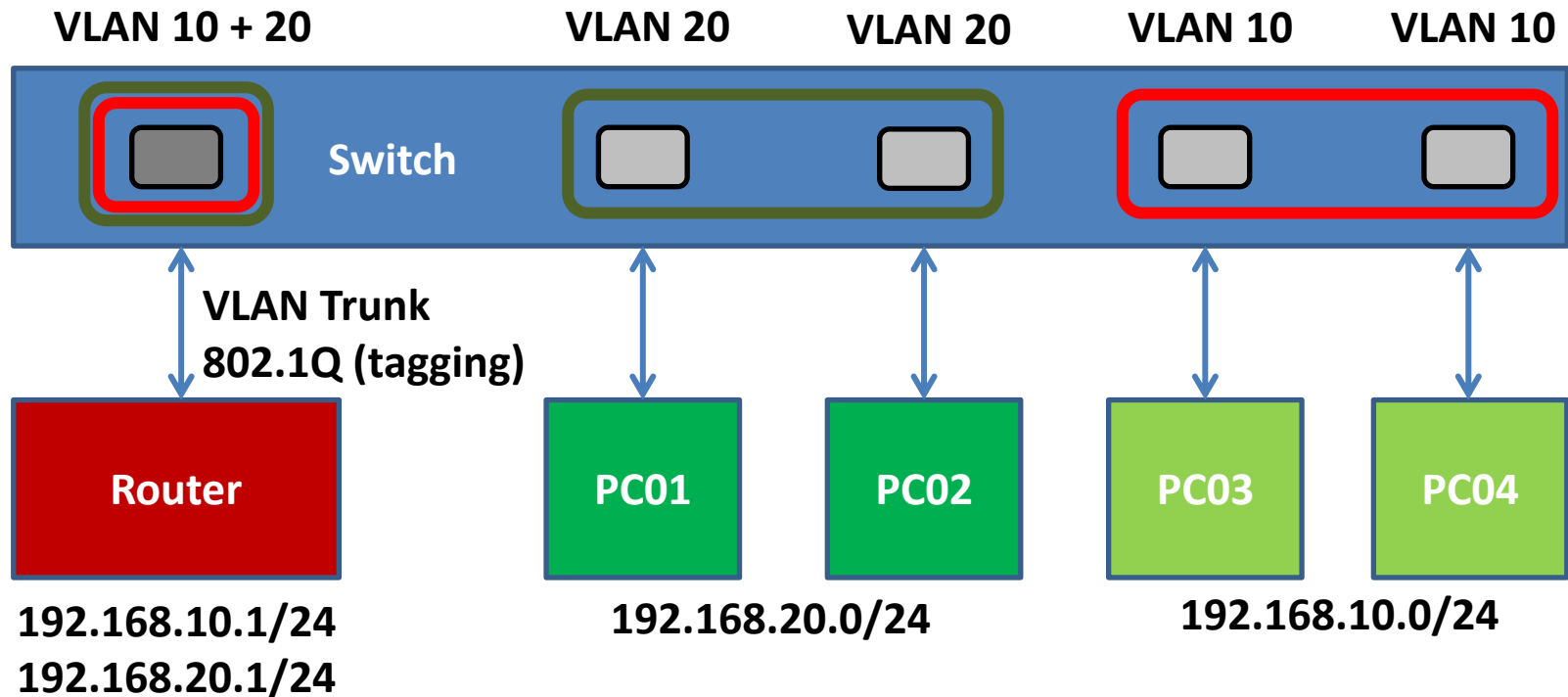
- Ein Computer in einem VLAN 10 kann nicht mit einem Computer in einem VLAN 20 kommunizieren.  
Über den Router werden die betreffenden VLANs über ein Interface im **Trunk** Modus verbunden. Dazu werden **VLAN Tags** verwendet.



# VLAN Grundlagen

VLANs werden über Layer3 mit Routing verbunden.

- VLANs können nur über **Routing** miteinander verbunden werden. Es benötigt daher einen Router oder einen **Layer 3** fähigen Switch (Multilayer Switch). Daher müssen sich alle VLANs in einem anderen IP-Netze befinden!



# Agenda



## «Sinn des VLAN Einsatzes»

# Gruppenarbeit «Sinn des VLAN Einsatzes»

- Teilt euch in 3-4er Gruppen ein.
- Schreibt auf ein Flipchartblatt verschiedene Einsatzzwecke (Sinn) von VLANs.
- Präsentiert eure Lösung anschliessend der Klasse.
- **20 Minuten Zeit für die Erarbeitung des Flipchartblattes.**

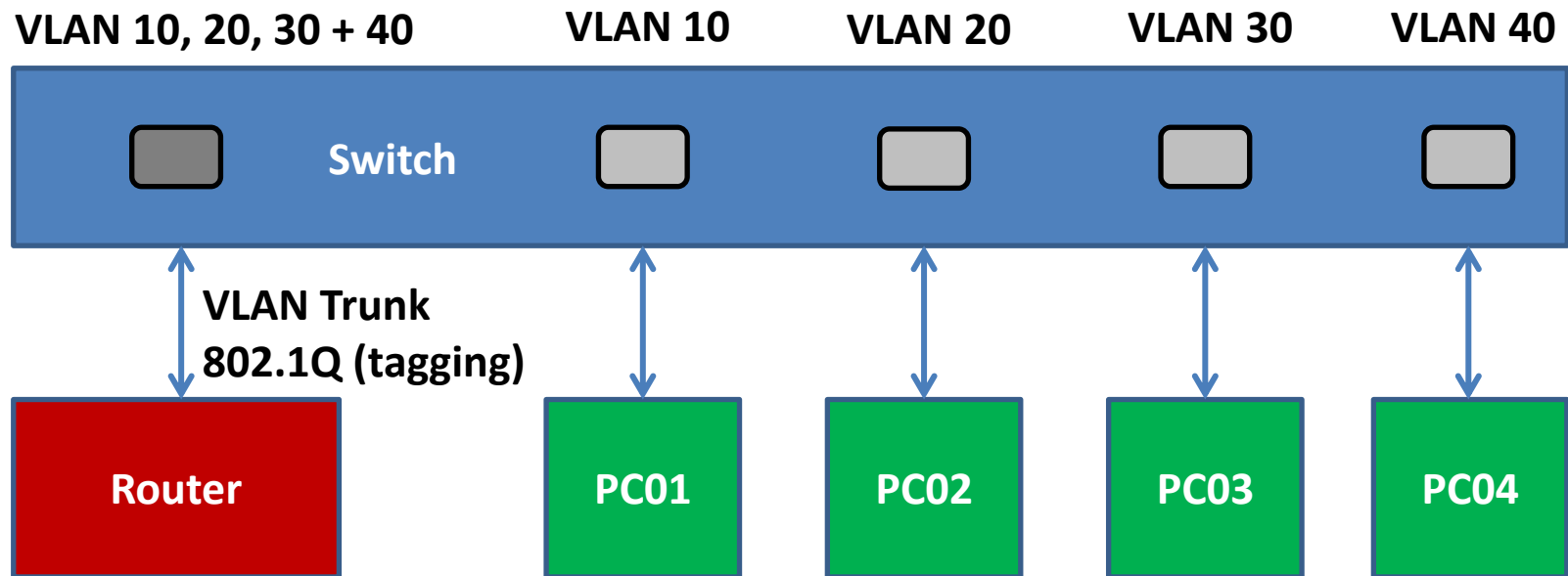
## **Ergebnisse der Arbeit:**

- ...



# VLAN Einsatz Security

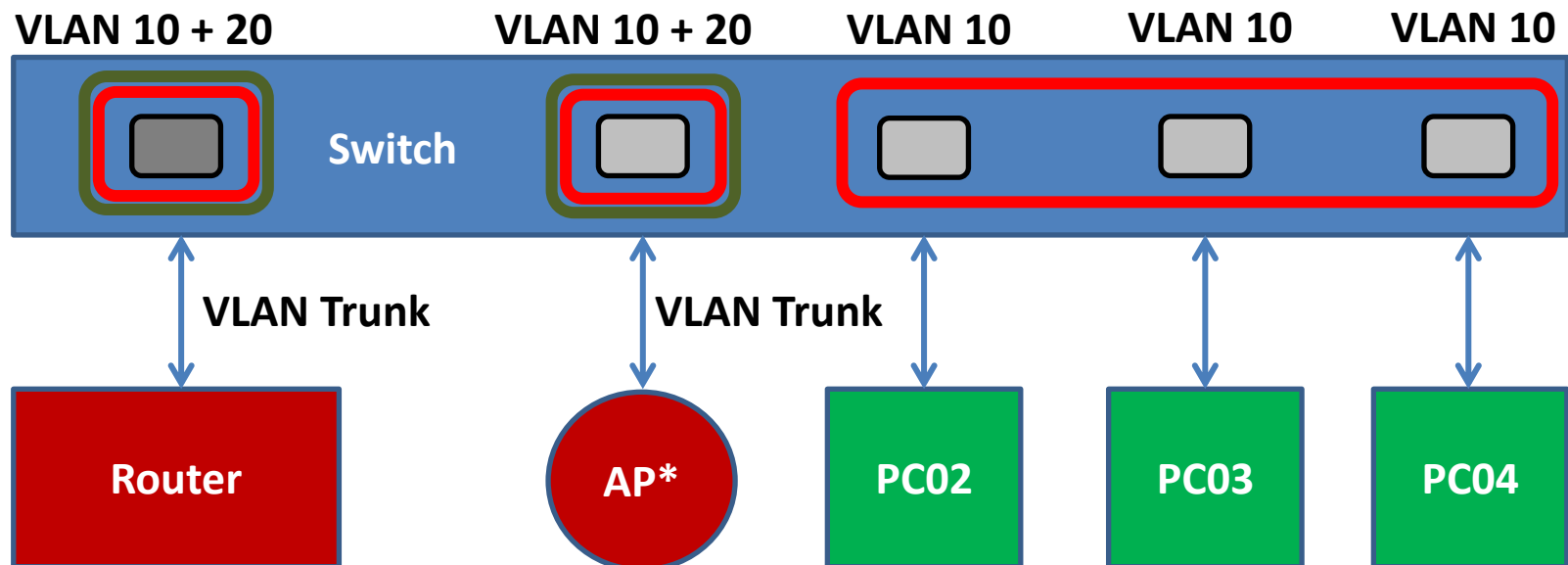
- Alle Computer sind in einem eigenen VLAN von allen anderen Computern getrennt (z.B. Internetcafé)



# VLAN Einsatz

## Verschiedene WLANs (SSID) über einen AP

- Es soll ein internes WLAN (SSID Intern) mit dem lokalen Netzwerk auf VLAN 10 verbunden werden. Zusätzlich wird ein vom lokalen Netzwerk getrenntes Gäste-WLAN (SSID Gast) nur mit dem Internet über VLAN 20 verbunden.



SSID: Intern (VLAN 10)

SSID: Gast (VLAN 20)

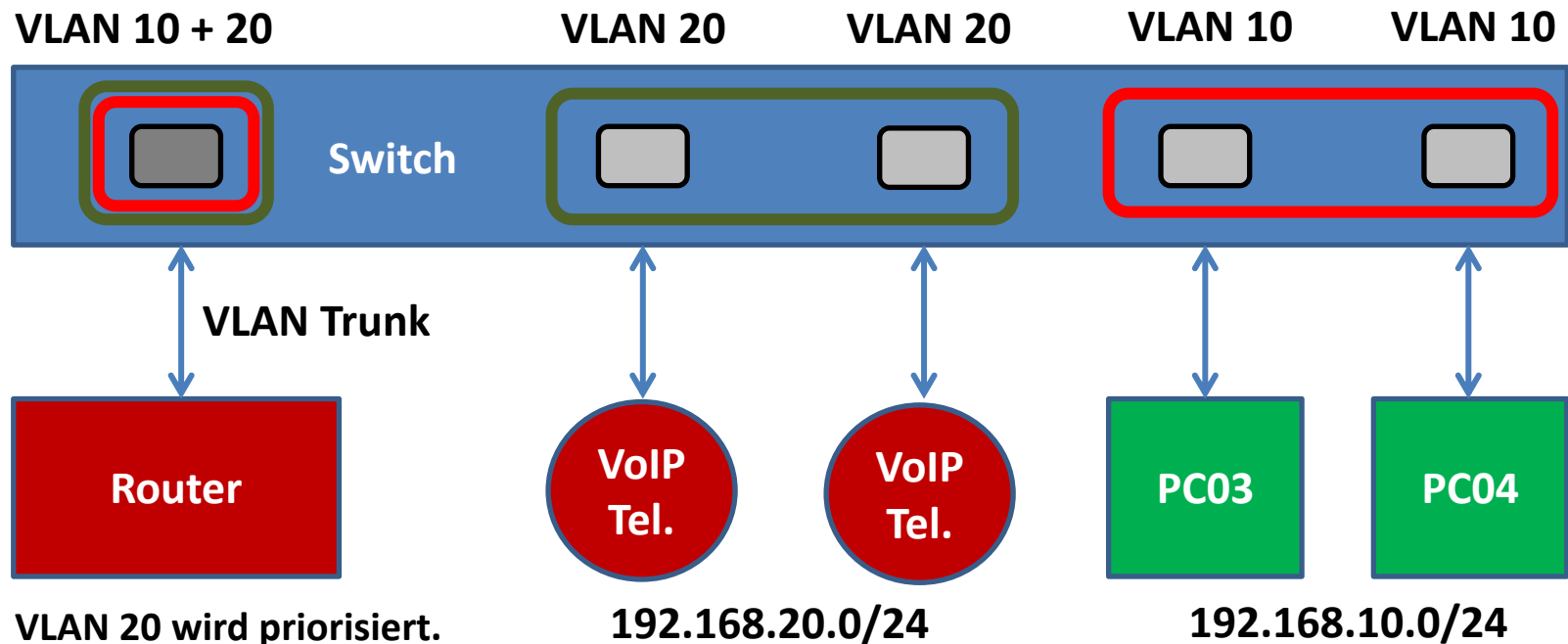
\* Access Point

© Mathias Gut - Jede Haftung im Zusammenhang  
mit diesen Inhalten ist ausgeschlossen!

# VLAN Einsatz

## Separierung und Priorisierung des VoIP Netzes

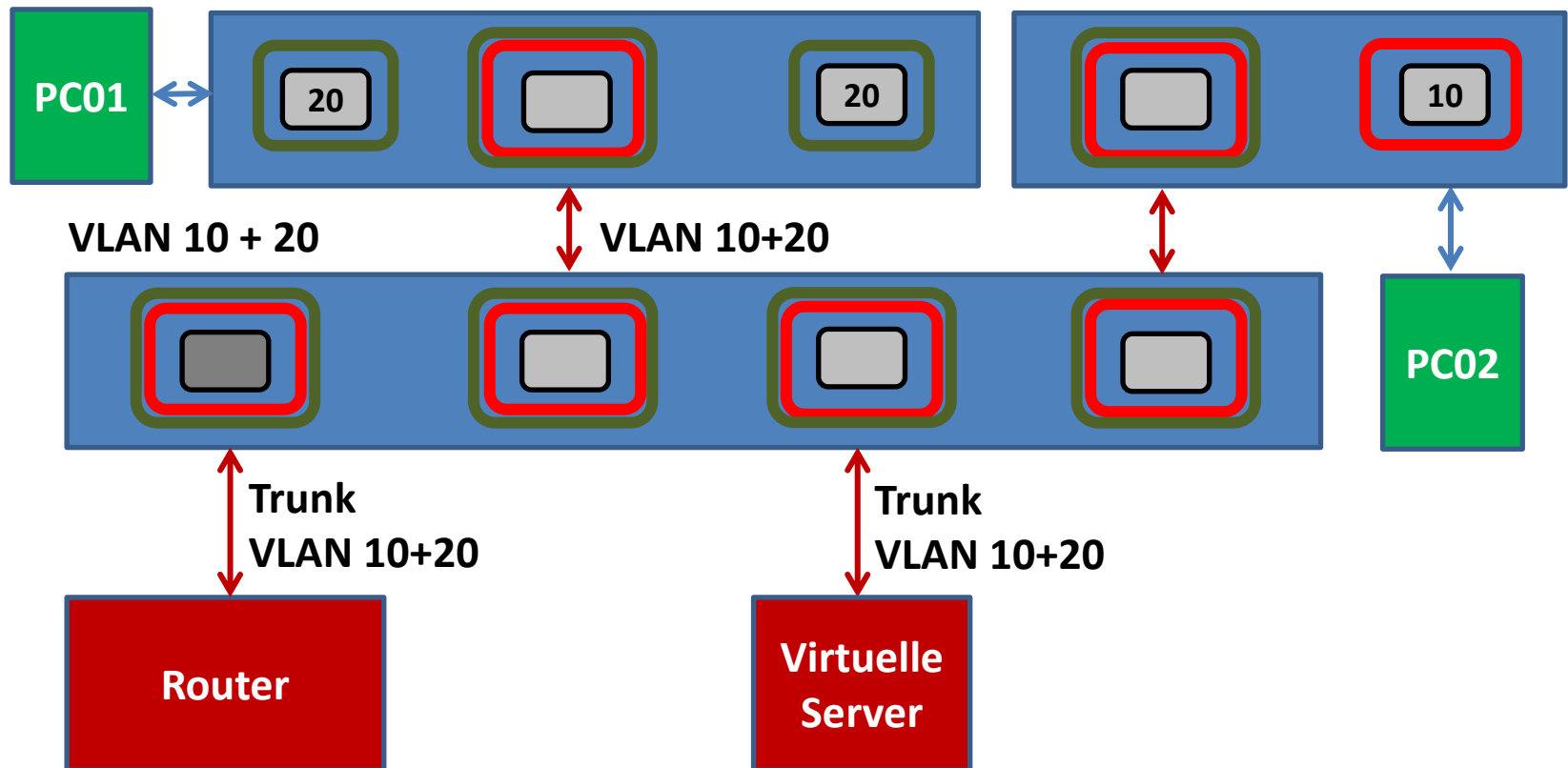
- Die VoIP Telefonie (VLAN 20) wird vom Datennetz (VLAN 10) getrennt. Das VLAN 20 wird dabei über den Router ins Internet priorisiert (QoS).



# VLAN Einsatz

## Stockwerk- oder Abteilungs-VLANs

- Pro Stockwerk (Abteilung) wird ein Switch mit einem eigenen VLAN eingesetzt. Dabei wird die Sicherheit erhöht und die Broadcasts minimiert.



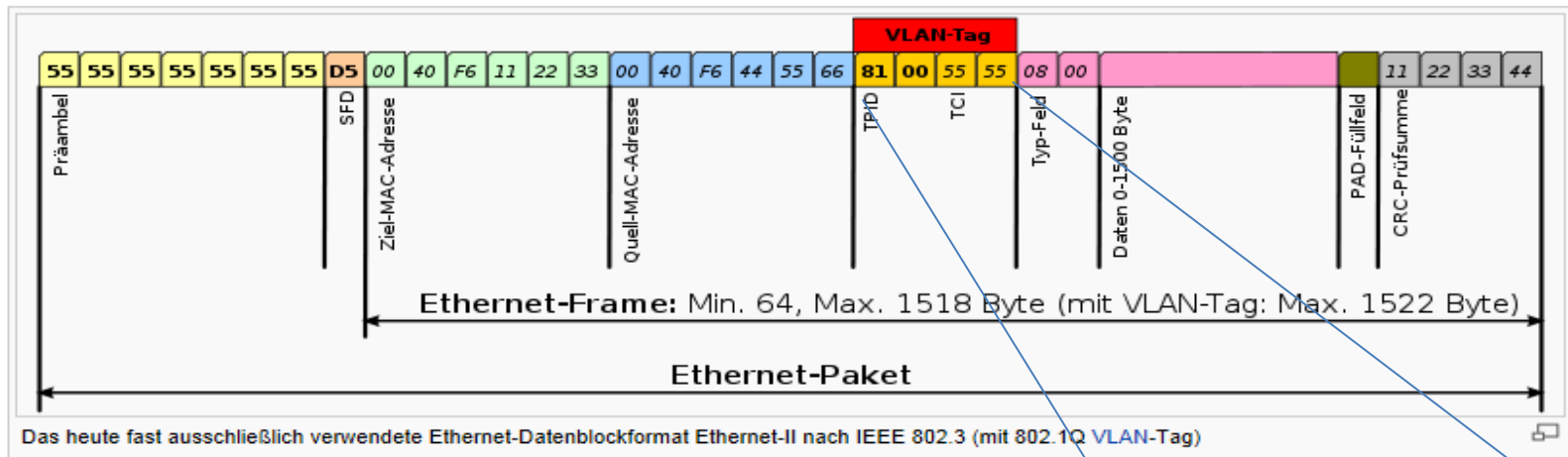
# Zusammenfassung Gründe für den VLAN-Einsatz

- Priorisierung möglich (QoS für VoIP)
- Verringerung CPU Overload (kleinere Broadcast Domänen)
- Verschiedene SSIDs auf einem Access Point
- Verringerung Sicherheitsrisiken (weniger Host sehen sich gegenseitig)
- Sicherheits-Konzept (sensible Daten in einem eigenen VLAN)
- Flexibler Design (Ordnung der Benutzer nach OU nicht nach Standort)
- Schnellere Problemlösung da weniger Geräte in einer Broadcast Domäne
- Arbeitsbelastung Rapid Spanning Tree (Rootbridge) durch Begrenzung geringer

# Repetition IEEE 802.3

## Beispiel Ethernet Frame

- Frames (Ethernet IEEE 802.3)



- Präambel / Start Frame Delimiter (aus kompatibilitätsgründen, diente der Synchronisation) (8 Byte – L1 Header)
- VLAN-Tag für die Definition von VLANs (4 Byte)
- Type Feld für die Definition des folgenden Protokolls auf höherer Schicht
- PAD Feld dient der Definition der Mindestgrösse von 64 Byte
- Trailer: CRC Prüfsumme / FCS-Feld - Frame Check Sequence (4 Byte)

Quelle Grafik: Wikipedia.org

16 bits	3 bits	1 bit	12 bits
TPID	TCI		
	PCP	DEI	VID

VID = VLAN-ID (4096 mögliche VLANs,  $2^{12}$ )

# Agenda

**«CLI Grundlagen  
Switch Installation»**

# Cisco Switch

## Grundkonfiguration

LAB>\_

### ***Beispiel 1 (Grundkonfiguration) :***

```
Switch>enable
```

```
Switch# configure terminal
```

```
Switch(config)# hostname Switch1 (Namen ändern)
```

```
S1(config)# enable secret cisco (Mit MD5 gesichertes  
Passwort)
```

```
S1(config)# service password-encryption (Verschlüsselt alle  
PW)
```



# Cisco Switch

## Grundkonfiguration

LAB>\_

### ***Switch IP Konfiguration:***

```
S1(config)# interface vlan 1
S1(config-if)# ip address 192.168.1.2 255.255.255.0
S1(config-if)# no shutdown
S1(config-if)# end
S1(config)# ip default-gateway 192.168.1.1
S1# write
```

### ***Switch IP entfernen:***

```
S1(config)# interface vlan 1
S1(config-if)# no ip address
S1(config-if)# shutdown
```

# Agenda



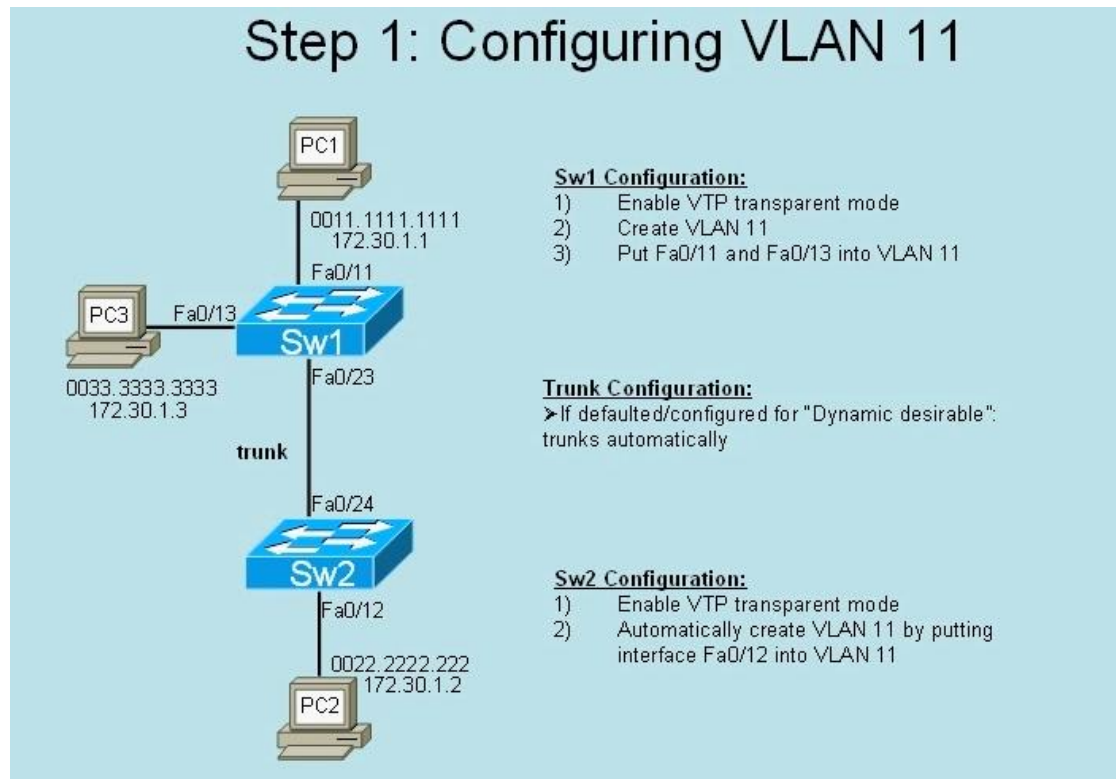
## «Cisco VLAN Konfiguration»

# Video anschauen

- CCENT/CCNA ICND1 100-101 Video
  - 4. VLANs

Video

Dauer: 10 Minuten



# Cisco Konfigurationsbeispiel

## „Access VLAN einrichten #1“

LAB>\_

**Beispiel 1 (Access VLAN erstellen):**

```
S1(config)# vlan 20
```

```
S1(config-vlan)# name Buchhaltung
```

```
S1(config)# interface fastethernet 0/2
```

```
S1(config-if)# switchport mode access
```

```
S1(config-if)# switchport access vlan 20 (erstellt VLAN 20)
```

```
S1(config)# interface range fastethernet 0/2 - 4
```

```
S1(config-if)# switchport mode access
```

```
S1(config-if)# switchport access vlan 20 (erstellt VLAN 20)
```

# Cisco Konfigurationsbeispiel

## „Access VLAN einrichten #2“

LAB>\_

*Beispiel 2 (Access VLAN erstellen):*

```
S1(config)# vlan 21
```

```
S1(config-vlan)# name Marketing
```

```
S1(config)# interface range fastethernet 0/10 - 12
```

```
S1(config-if)# switchport access vlan 21
```

```
S1#show vlan brief (VLANs Zusammenfassung ansehen)
```

```
S1# show interface vlan 20
```

```
S1#show interface trunk (Trunk Ports anzeigen)
```

```
S1#show vlan (VLANs ansehen / mehr Details)
```

# Cisco Konfigurationsbeispiel

## „VLAN Trunk 802.1Q einrichten“

LAB>\_

### **Port für Trunking nach 802.1Q einrichten:**

```
S1(config)# interface fastethernet 0/10
S1(config-if)# description Trunk zu SW1 (optional)
S1(config-if)# switchport trunk encapsulation dot1q
S1(config-if)# switchport mode trunk
```

### **VLAN Trunk auf ein Portrange:**

```
S1(config)# interface range fastethernet 0/10 - 11
S1(config-if)# description Trunk zu SW3 (optional)
S1(config-if-range)# switchport trunk encapsulation dot1q
S1(config-if-range)# switchport mode trunk
```

# Cisco Konfigurationsbeispiel

## „VLAN Trunk 802.1Q Switchport Mode“

LAB>\_

### Switchport Modus wählen:

```
S1(config)# interface fastethernet 0/10
```

```
S1(config)# interface range fastethernet 0/10 - 11
```

```
S1(config-if)# switchport trunk encapsulation dot1q
```

```
S1(config-if)# switchport mode access (nur Access)
```

```
S1(config-if)# switchport mode trunk (nur Trunk)
```

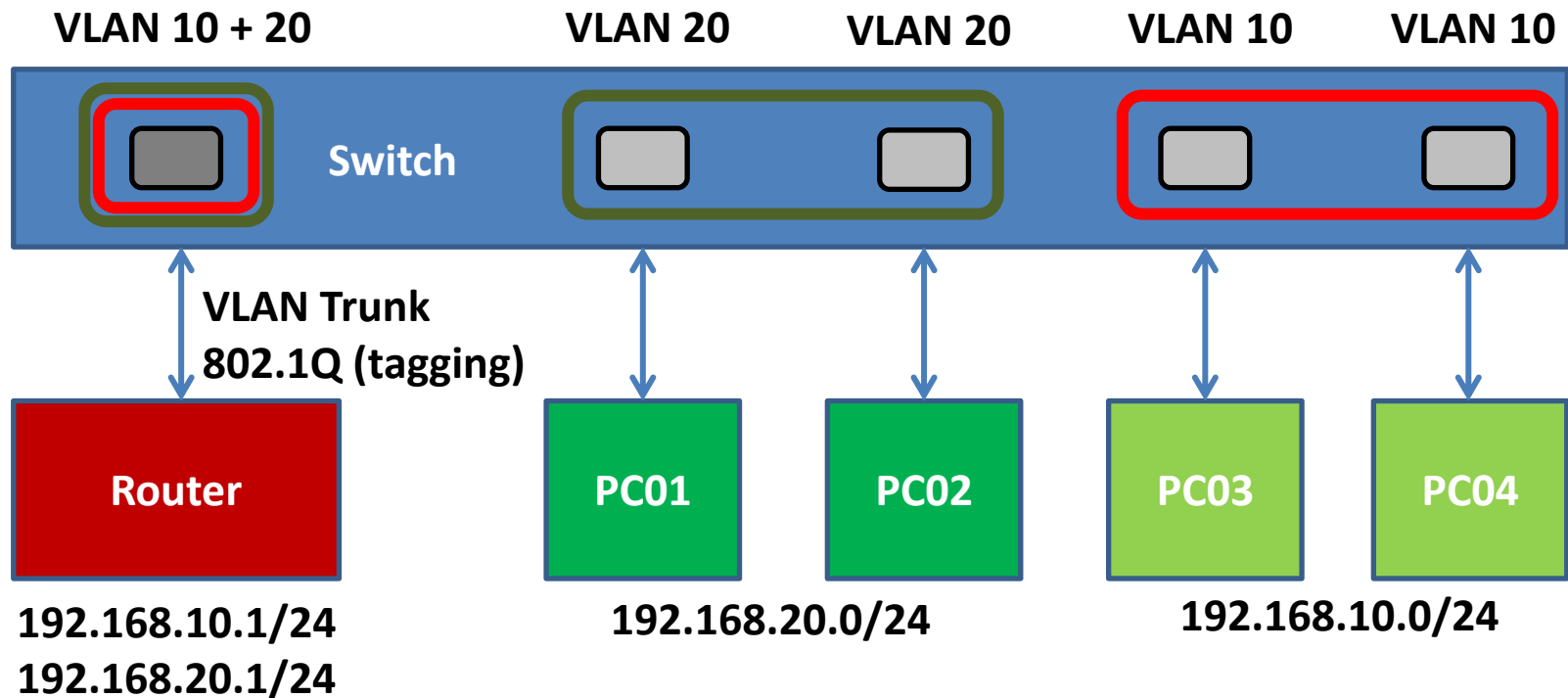
```
S1(config-if)# switchport mode dynamic auto (Access o. Trunk)
```

```
S1(config-if)# switchport mode dynamic desirable (Access o.  
Trunk)
```

# VLAN Grundlagen

VLANs werden über Layer3 mit Routing verbunden.

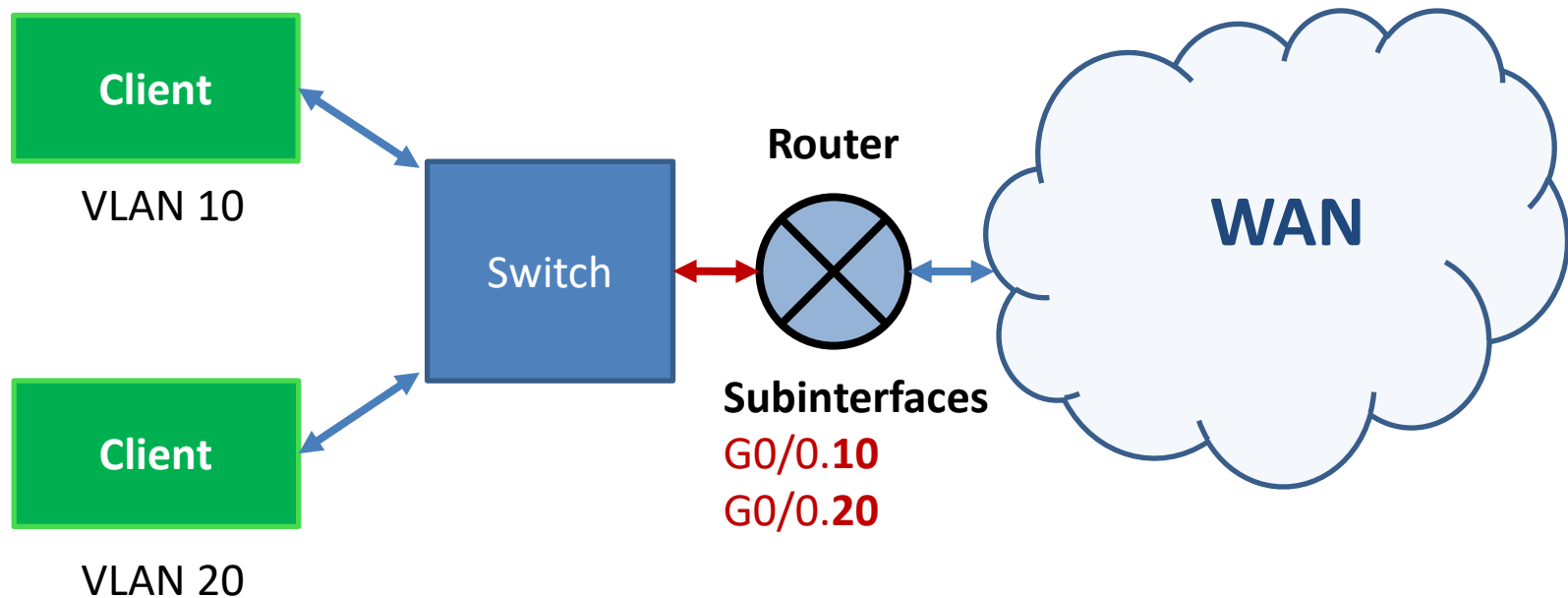
- VLANs können nur über **Routing** miteinander verbunden werden. Es benötigt daher einen Router oder einen **Layer 3** fähigen Switch. Daher müssen sich alle VLANs in einem anderen IP-Netze befinden!





# Inter-VLAN Routing (optional)

## Router on a Stick «RoaS»



**Zur besseren Übersicht werden bei den Subinterfaces die VLAN-IDs für die Nummerierung verwendet.**

# Erklärung

## Router on a Stick «RoaS»

Ein "**Router on a Stick**" ist eine Netzwerktopologie, bei der ein einzelner Router über eine einzige physische Schnittstelle mit einem Switch verbunden ist, um den Verkehr zwischen mehreren VLANs zu routen.

### Funktionsweise:

#### 1. Trunk-Verbindung:

- Die Verbindung zwischen dem Router und dem Switch wird als **Trunk-Port** konfiguriert.
- Dieser Trunk-Port kann Datenverkehr für mehrere VLANs transportieren.

#### 2. Subinterfaces auf dem Router:

- Da der Router nur eine physische Schnittstelle hat, werden **logische Subinterfaces** für jedes VLAN erstellt.
- Jedes Subinterface wird mit einer IP-Adresse aus dem entsprechenden VLAN versehen.

#### 3. Inter-VLAN-Routing:

- Der Router empfängt getaggte VLAN-Pakete, verarbeitet sie und sendet sie an das Ziel-VLAN zurück.
- Dadurch können Geräte in verschiedenen VLANs miteinander kommunizieren.

### Vorteile:

- Kostengünstig, da nur ein Router mit einer einzelnen Schnittstelle benötigt wird.
- Einfach für kleinere Netzwerke mit begrenzten VLANs.

### Nachteile:

- Leistungslimitierung, da der gesamte VLAN-Verkehr über eine einzige physische Verbindung läuft (Flaschenhals).
- Nicht ideal für große Netzwerke mit hohem Datenaufkommen.

### Einsatzbereiche:

- Kleine bis mittelgroße Netzwerke mit wenigen VLANs.
- Testumgebungen oder Schulungsnetzwerke.

# Cisco Konfigurationsbeispiel (optional)

## «Roas Inter-VLAN Routing»

LAB>\_

### **VLAN 10:**

```
R1(config)# interface gigabitethernet 0/0.10
R1(config-subif)# encapsulation dot1Q 10
R1(config-subif)# ip address 10.1.1.254 255.255.255.0
```

### **VLAN 20:**

```
R1(config)# interface gigabitethernet 0/0.20
R1(config-subif)# encapsulation dot1Q 20
R1(config-subif)# ip address 10.2.1.254 255.255.255.0
.....
```

**Vorsicht! Alle VLANs werden nun untereinander geroutet! Um dies zu verhindern müssen ACLs genutzt werden.**

## Ende Block 6

«Ende»

# Lernziele des 6. Modulblocks

- **Du kannst...**

1. ...die Grundlagen von VLANs (802.1Q) im Zusammenhang mit Netzwerkdesigns einordnen.
2. ...verschiedene Einsatzzwecke von VLANs erläutern.
3. ...einen Switch grundlegend konfigurieren.
4. ...VLANs auf Basis von 802.1Q selbstständig konfigurieren.

# Deine Hausaufgaben

## Stoff Nachbearbeitung 6. Modul:

- **Repetition der Folieninhalte des Modulblocks:** Ergänzen deiner individuellen Zusammenfassung.
- **Lernstoff Vertiefung:**
  - CCNA1 Buch Kapitel 5 «Analyzing Ethernet LAN Switching»
  - CCNA1 Buch Kapitel 6 «Configuring Basic Switch Management»
  - CCNA1 Buch Kapitel 8 «Implementing Ethernet Virtual LANs»
- **Lernvideos «Youtube»:**

Suche ein gutes Lernvideo über Switching und nimm deinen Vorschlag in den Unterricht für den gemeinsamen Austausch mit.
- **Praxistransfer:**

Erstelle mit dem CISCO Pakettracer ein Beispiel-Netzwerkdesign. Konzentriere dich dabei auf das Switching. Wir besprechen im Unterricht gemeinsam die verschiedenen Designvorschläge, Konzeptvorgaben und eigenen Erfahrungen. Du kannst dazu ein bekanntes Beispielnetzwerk verwenden oder ein eigenes Beispiel entwickeln.

  - Mache bei allen Switchen eine Grundkonfiguration gemäss den Folieninhalten. Nutze dabei die aus deiner Sicht sinnvollen Geräte im Pakettracer auch wenn die «simulierten» CISCO Switche nicht mehr aktuell sind. «Konzentriere Dich vor allem auf das Design.»
  - Beantworte mindestens folgende Fragen:
    - Beachtest du unternehmenseigene Vorgaben beim Konzept?
    - Was ist dir im Konzept wichtig?
    - Wo siehst du die Herausforderungen?
    - Verwendest du dabei VLANs nach 802.1Q?
    - Weist dein Switch-Design Redundanzen auf und ist so vor Ausfällen von Netzwerkverbindungen und Switchen geschützt?
  - Welche Switches verwendet ihr in eurem Unternehmen und wie werden diese konfiguriert, verwaltet und überwacht?
- **Vorbereitung auf das nächste Modul:**
  - CCNA1 Buch Kapitel 9 «Spanning Tree Protocol Concepts» Verschaffe dir hier nur eine kurze Übersicht betreffend STP. Die Vertiefung der Thematik erfolgt erst im Nachfolgemodul – «NPDO - Netzwerk, Planung, Design und Optimierung»