|  |
| --- |
| VS-Projekt IT11a |
| Gruppe 4 |
| Benedikt Kowatsch, Tim Mücke, Christian Werder, Markus Hölzle |

|  |
| --- |
|  |

[Theorie: 3](#_Toc13048647)

[IP-Adressierungsschema: 3](#_Toc13048648)

[VLANing: 3](#_Toc13048649)

[ActiveDirectory: 3](#_Toc13048650)

[Konfiguration: 4](#_Toc13048651)

[Router: 4](#_Toc13048652)

[Switch 5](#_Toc13048653)

[Optionale Erweiterungen zum Netz (geplant): 7](#_Toc13048654)

# **Theorie:**

## IP-Adressierungsschema:

**Beschreibung:**

Wir haben uns für den privaten Klasse A-Netzbereich entschieden. Unsere IP-Adresse setzt sich wie folgt zusammen:

Im ersten Oktett wird die 10 verwendet (privates netz).

Als zweites Oktett nutzen wir die 4, da wir Gruppe 4 sind.

Das dritte Oktett kennzeichnet in welchem VLAN sich der PC befindet.

Im letzten Oktett wird der angeschlossene Port des Switches genutzt.

Um die VLANs zu subnettieren benutzen wir eine /24 (255.255.255.0) Subnetzmaske.

Falls das Gerät nicht direkt an einen Port des Switches angeschlossen wird, gilt eine andere Regelung.

Die Subinterfaces des Routers erhalten im vierten Oktett die 254.

Da der WLAN-Access-Point logisch (ersichtlich) von den direktverbundenen Geräten getrennt werden soll, wird dieser auf Port 13 des Switches gesteckt.

Die verbundenen Geräte sollen aus einem IP-Adress-Pool zwischen 15 und 100 gespeist werden.

**Beispiel:**

PC1: 10.4.10.1 /24 Gateway: 10.4.10.254 /24

## VLANing:

**Beschreibung:**

Damit die Arbeitsplätze nicht untereinander kommunizieren können, werden sie in eigene VLANs aufgenommen. Damit sie aber trotzdem den Server und das Internet erreichen wird ein Router-on-a-Stick im Netz konfiguriert. Dieser Arbeitet mit Access-Listen um die Zugriffsmöglichkeiten zu regeln. Wir verwenden VLAN 10 - 40 für die Arbeitsplätze und das VLAN 100 für den Server. Das VLAN 99 dient als Management-VLAN (z. B. SSH-Zugriffe).

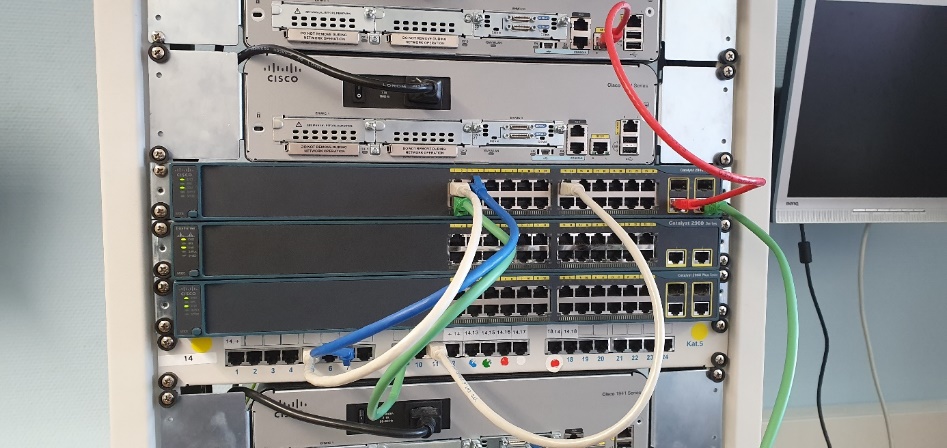
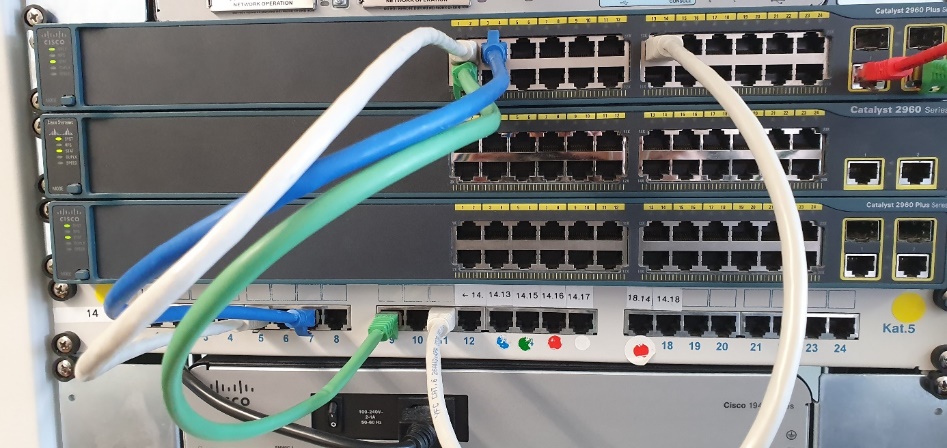
## ActiveDirectory:

**Beschreibung:**

Auf dem Windows-Server haben wir einen Domain-Controller installiert. Dieser ist mit einem auf dem Server installierten DNS-Dienst verknüpft. Als Domain haben wir uns für gruppe4.de entschieden. In unserem ActiveDirectory haben wir eine Gruppe und 4 Benutzer angelegt.

Die Benutzer wurden alle der Gruppe hinzugefügt. Dadurch entsteht die Möglichkeit, Ressourcen auf einzelne Benutzer einzuschränken. Wie z. B. die Ordnerfreigabe die wir auf dem Server eingerichtet haben. Diese wurde so eingerichtet, dass nur Mitglieder aus der Gruppe „Gruppe4“ darauf Zugriff haben. Die Ordnerfreigabe ersetzt die Aufgaben/Funktion eines TFTP-Servers.

# Aufbau:





Im oberen Bild sieht man wie die PCs auf dem Switch eingesteckt sind.  
Man kann deutlich die logische Trennung zwischen PCs und

WLAN-Accesspoint erkennen. Rechts sieht man wie der Router   
(rotes Kabel) mit einem Uplink-Port des Switches verbunden ist.  
Der andere Uplink-Port (grünes Kabel) ist mit dem Server verbunden.

Auf dem Gigabit 0/0 Port (roter Kreis) des Routers wurde später der  
Internetzugang (FritzBox) angeschlossen.

# **Konfiguration:**

## Router:

hostname MartinRouterKing

domain Name einrichten:

ip domain-name gruppe4.de

ssh einrichten:

username admin secret admin

line vty 0 15

transport input ssh

login local

exit

ip ssh version 2

access Liste erstellen:

access-list 10 permit 10.4.100.0 0.0.0.255

access-list 10 deny 10.4.0.0 0.0.255.255

access-list 10 permit all

access-list 1 permit 10.4.0.0 0.0.255.255

subinterfaces für einzelne VLANs konfigurieren und NAT konfigurieren:

interface GigabitEthernet 0/1.10

encapsulation dot1Q 10

ip address 10.4.10.254 255.255.255.0

ip nat inside

ip access-group 10 out

exit

interface GigabitEthernet 0/1.20

encapsulation dot1Q 20

ip address 10.4.20.254 255.255.255.0

ip nat inside

ip access-group 10 out

exit

interface GigabitEthernet 0/1.30

encapsulation dot1Q 30

ip address 10.4.30.254 255.255.255.0

ip nat inside

ip access-group 10 out

exit

interface GigabitEthernet 0/1.40

encapsulation dot1Q 40

ip address 10.4.40.254 255.255.255.0

ip nat inside

ip access-group 10 out

exit

interface GigabitEthernet 0/1.100

encapsulation dot1Q 100

ip address 10.4.100.254 255.255.255.0

ip nat inside

exit

interface GigabitEthernet 0/1

ip address 10.4.99.254 255.255.255.0

no shutdown

exit

interface GigabitEthernet 0/0

ip address 192.168.10.4 255.255.255.0

ip nat outside

no shutdown

exit

statische Route zur Fritzbox konfigurieren:

ip route 0.0.0.0 0.0.0.0 192.168.10.254

Switch:

Hostname festgelegt: Der\_Switcher

hostname Der\_Switcher

Ssh einrichten:

crypto key generate rsa

1024

username admin secret admin

line vty 0 15

transport input ssh

login local

exit

ip ssh version 2

VLANs einrichten und IP Adressen konfigurieren:

vlan 99

name Management

exit

vlan 100

name Server

exit

vlan 10

exit

vlan 20

exit

vlan 30

exit

vlan 40

name //TODO:\_WirelessAP

exit

interface vlan 99

ip address 10.4.99.1 255.255.255.0

exit

interface vlan 10

ip address 10.4.10.253 255.255.255.0

exit

Trunk konfigurieren:

interface GigabitEthernet 0/1

switchport mode trunk

switchport trunk native vlan 99

switchport trunk allowed vlan 99,100,10,20,30,40

exit

Alle FE Ports herunterfahren:

interface range FastEthernet0/1-24

shutdown

exit

Benötigte FE Ports hochfahren und als Access Ports verwenden:

interface FastEthernet 0/1

switchport mode access

switchport access vlan 10

no shutdown

exit

interface FastEthernet 0/2

switchport mode access

switchport access vlan 20

no shutdown

exit

interface FastEthernet 0/3

switchport mode access

switchport access vlan 30

no shutdown

exit

interface FastEthernet 0/13

switchport mode access

switchport access vlan 40

no shutdown

exit

Default Gateway eingerichtet:

ip default-gateway 10.4.99.254

# **Optionale Erweiterungen zum Netz (geplant):**

Sticky-MAC-Addresses, DTP Deaktivieren, DHCP verwenden, SSH einrichten für Switch und Router, Firewall einrichten, Port-Security, Fileshare auf Server,