Titel: Labor05 – VLANs

Klasse: 4BHIF

Name: Haiden

Gruppe: 01

Aufgabe: 15.12.2020 Abgabe: 12.01.2021

Inhaltsverzeichnis

[1 Theorie-Teil VLANs 1](#_Toc61311112)

[1.1 Allgemeines 1](#_Toc61311113)

[1.2 Vorteile gegenüber geswitchten Netzen 1](#_Toc61311114)

[1.3 VLAN-Typen: Portbased vs Tagged VLANs 1](#_Toc61311115)

[1.3.1 Portbasiert 1](#_Toc61311116)

[1.3.2 Tagged VLANs 1](#_Toc61311117)

[1.4 Statisches vs. Dynamisch 2](#_Toc61311118)

[1.4.1 Statisch 2](#_Toc61311119)

[1.4.2 Dynamisch 2](#_Toc61311120)

[2 VLAN-Konfiguration 3](#_Toc61311121)

[2.1 Erstellen der Trunkverbindung (letzter Port). Kontrolle mittels CDP 3](#_Toc61311122)

[2.1.1 Trunk einschalten 3](#_Toc61311123)

[2.2 Konfiguration der VTP Clients & Server und erstellen der Domäne IFDOM 4](#_Toc61311124)

[2.2.1 Konfiguration von Switch0 als Server 4](#_Toc61311125)

[2.2.2 Konfiguration von Switch1 als Client 4](#_Toc61311126)

[2.3 Status anzeigen 4](#_Toc61311127)

[2.3.1 Switch0 4](#_Toc61311128)

[2.3.2 Switch1 5](#_Toc61311129)

[2.4 Erstellen der VLANs 5](#_Toc61311130)

[2.4.1 Verkauf-VLAN erstellen 5](#_Toc61311131)

[2.4.2 Einkaufs-VLAN erstellen 5](#_Toc61311132)

[2.5 Zuweisen der Ports 6](#_Toc61311133)

[2.5.1 Switch0 6](#_Toc61311134)

[2.5.2 Switch1 6](#_Toc61311135)

[2.6 Anzeige und Analyse der Konfiguration 7](#_Toc61311136)

[2.6.1 Switch0\_Etage1 7](#_Toc61311137)

[2.6.2 Switch1\_Etage2 7](#_Toc61311138)

[2.7 Ping-Test 8](#_Toc61311139)

[3 Inter-VLAN Routing 9](#_Toc61311140)

[3.1 Konfiguration: 9](#_Toc61311141)

[3.1.1 Für VLAN 10 9](#_Toc61311142)

[3.1.2 FÜR VLAN 20: 10](#_Toc61311143)

[3.2 Ping Test 10](#_Toc61311144)

[4 Management\_Fernwartung 12](#_Toc61311145)

[4.1 VLAN Konfiguration an allen 3 Switches 12](#_Toc61311146)

[4.1.1 Switch0 – Core-Switch 12](#_Toc61311147)

[4.1.2 Switch1 12](#_Toc61311148)

[4.1.3 Switch2 12](#_Toc61311149)

[4.2 SSH Zugang einrichten 13](#_Toc61311150)

[4.2.1 Switch0 13](#_Toc61311151)

[4.2.2 Switch1 13](#_Toc61311152)

[4.2.3 Switch2 14](#_Toc61311153)

[4.3 Testen Sie den Zugriff. Von welchen PC’s können sie zugreifen? Ist das zufriedenstellen? 15](#_Toc61311154)

[4.4 Konfigurieren Sie den Coreswitch als VTP Server (Domäne NVSDom) 15](#_Toc61311155)

[4.5 Konfigurieren der Switches und Trunk-Verbindungen 15](#_Toc61311156)

[4.5.1 Core-Switch 15](#_Toc61311157)

[4.5.2 Switch 1 17](#_Toc61311158)

[4.5.3 Switch 2 17](#_Toc61311159)

[4.6 VLAN 10 als Client-VLAN einrichten 17](#_Toc61311160)

[4.6.1 Am Core-Switch 17](#_Toc61311161)

[4.6.2 Switch 1 17](#_Toc61311162)

[4.6.3 Switch 2 17](#_Toc61311163)

[4.7 Ports auf das VLAN setzen 18](#_Toc61311164)

[4.7.1 Switch1 18](#_Toc61311165)

[4.7.2 Switch 2 18](#_Toc61311166)

[4.8 SSH Zugriff testen 19](#_Toc61311167)

# Theorie-Teil VLANs

Quellen:

<https://www.ip-insider.de/was-ist-vlan-a-598987/>

<https://de.wikipedia.org/wiki/Virtual_Local_Area_Network>

## Allgemeines

Mit VLANs kann man physische Netzwerke in voneinander isolierte, logische Teilnetze aufteilen und so sauber voneinander trennen. So kann man mit VLANs Organisationsstrukturen in einem Unternehmen abbilden, ohne zusätzliche Geräte benötigen zu müssen. VLANs bringen eine Reihe an Vorteilen und eine sehr gefragte Flexibilität mit, ein Beispiel:

Wechselt ein Mitarbeiter seinen Standort, so kann er seine Geräte ganz einfach weiterbenutzen. Der Administrator ändert hierfür einfach den Netzwerkport. Wechseln Mitarbeiter ihre Abteilung, so kann der Administrator mit einem Klick einen neues, für die Abteilung gedachtes VLAN dem bisher genutzten Netzwerk-Port zuweisen.

## Vorteile gegenüber geswitchten Netzen

Mit VLANs kann man sensible, interne Services von öffentlichen Services wie öffentlichen Webservern trennen.

Hierbei gelten VLANs robuster als geswitchte, physische Netze. Geswitchte Netze sind anfällig für MAC-Flooding und MAC-Spoofing.

VLANs haben nicht nur Sicherheitsvorteile, man kann sich durch die Nutzung derer auch einen Bandbreitengewinn für zeitkritische, wichtige Anwendungen wie VoIP herausschlagen. So kann man VoIP Traffic über dedizierte, priorisierte WLANs abwickeln, um so eine reibungslose Kommunikation zu gewährleisten. Sie können auch dafür genutzt werden, Broadcastdomänen innerhalb eines Netzes zu verkleinern, dies hat zur Folge, dass Anfragen nicht mehr über das ganze Netz übermittelt werden (müssen), sondern nur mehr in den logischen, kleineren Teilnetzen. So kann eine defekte Netzwerkkarte durch z.B. Broadcaststürme nicht mehr das ganze Netzwerk lahmlegen, sondern nur mehr ein logisches VLAN.

## VLAN-Typen: Portbased vs Tagged VLANs

### Portbasiert

Sie sind die Urform der VLANs. Ein physisches Netzwerk wird mit mehreren managebaren Switchen in mehrere logische Teilnetzwerke aufgeteilt, in dem einem Ethernet Port ein VLAN zugeordnet wird. Sind im Frame Tags vorhanden, werden diese vom Switch entfernt, bevor dieser das Paket weitersendet, in der Fachsprache nennt man dies einen „untagged“ Port. Portbasierte VLANs sind auch über mehrere Switches hin ausdehnbar. Zur Kommunikation zwischen den einzelnen Switches wird ein Trunk Port verwendet.

### Tagged VLANs

Tagged VLANs verwenden Netzwerkpakete, die in ihrem Datenblockformat die VLAN ID / Nummer eingebaut, also eine VLAN Markierung, haben. Zu dieser Gattung gehört das offene Format IEEE 802.1Q, aber auch propieretäre Formate wie SPB (Shortest Path Bridging), Cisco ISL und 3Com VLT.

Bei Paketen, die kein VLAN Tag besitzen, wird vom dem Weiterleiten über einen Trunk ein VLAN-Tag hinzugefügt, damit der Switch auf der Empfängerseite weiß, in welches VLAN er das Paket weiterleiten muss. Empfängt ein Switch auf einem VLT-Port (Trunkport) einen Frame mit VLAN-Tag nach IEEE 802.1q, kann auch dieser es unverändert weiterleiten. Lediglich der Switch am Empfangsport muss unterscheiden, ob er ein Tagging-fähiges Endgerät beliefert (dann kann der Frame unverändert bleiben) oder ob es sich um ein nicht Tagging-fähiges Endgerät handelt, welches zu dem aktuellen VLAN gehört (dann ist das Tag zu entfernen). Hierzu muss die zugehörige VLAN-ID im Switch hinterlegt sein. Da nach IEEE 802.1Q alle Pakete mit VLAN-Tags markiert sind, müssen einem Trunk entweder alle VLAN-IDs, die er weiterleiten soll, hinterlegt werden, oder er ist zur Weiterleitung aller VLANs konfiguriert. Werden Pakete ohne Tag auf einem Trunk-Port empfangen, können diese je nach Konfiguration entweder einem Default-VLAN zugeordnet werden (der Switch bringt das Tag nachträglich an), oder sie werden verworfen.

## Statisches vs. Dynamisch

### Statisch

Hier wird einem Port eines Switches fest eine VLAN-Konfiguration zugeordnet. Er gehört dann zu einem *Port-basierten VLAN*, zu einem *untagged VLAN* oder er ist ein Port, der zu mehreren VLANs gehört. Die Konfiguration eines Ports ist bei statischen VLANs fest durch den Administrator vorgegeben. Sie hängt nicht vom Inhalt der Pakete ab und steht im Gegensatz zu den dynamischen VLANs unveränderlich fest. Damit ist eine Kommunikation des Endgerätes an einem Port nur noch mit den zugeordneten VLANs möglich. Gehört ein Port zu mehreren VLANs, ist er ein VLAN-Trunk und dient dann meist zur Ausdehnung der VLANs über mehrere Switches hinweg.

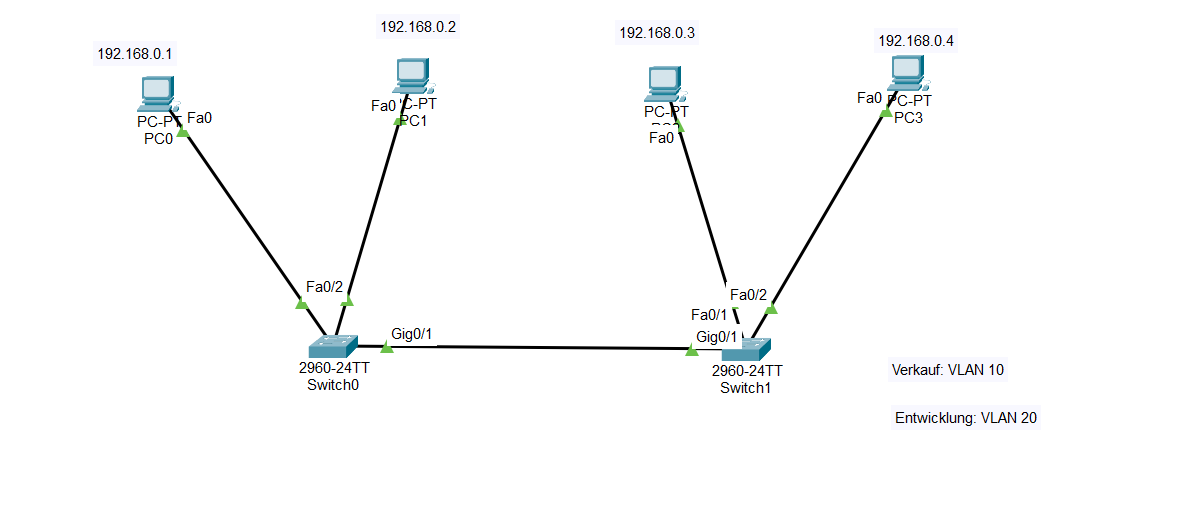
Durch die Möglichkeit, einen Port mehreren VLANs zuzuordnen, können zum Beispiel auch Router und Server über einen einzelnen Anschluss an mehrere VLANs angebunden werden, ohne dass für jedes Teilnetz eine physische Netzwerkschnittstelle vorhanden sein muss. Somit kann ein einzelnes Gerät – auch ohne Router – seine Dienste in mehreren VLANs anbieten, ohne dass die Stationen der verschiedenen VLANs miteinander kommunizieren können.  
Diese VLAN-Trunks dürfen nicht mit den Trunks im Sinne von Link Aggregation verwechselt werden, bei denen mehrere physische Übertragungswege zur Durchsatzsteigerung gebündelt werden.

### Dynamisch

Bei der dynamischen Implementierung eines VLANs wird die Zugehörigkeit eines Frames zu einem VLAN anhand bestimmter Inhalte des Frames getroffen. Da sich alle Inhalte von Frames praktisch beliebig manipulieren lassen, sollte in sicherheitsrelevanten Einsatzbereichen auf den Einsatz von *dynamischen VLANs* verzichtet werden. *Dynamische VLANs* stehen im Gegensatz zu den *statischen VLANs*. Die Zugehörigkeit kann beispielsweise auf der Basis der MAC- oder IP-Adressen geschehen, auf Basis der Protokoll-Typen oder auch auf Anwendungsebene.

Durch Dynamische VLANs kann zum Beispiel auch erreicht werden, dass ein mobiles Endgerät immer einem bestimmten VLAN angehört – unabhängig von der Netzwerkdose, an die es angeschlossen wird. Eine andere Möglichkeit besteht darin, einen bestimmten Teil des Datenverkehrs wie zum Beispiel VoIP aus Performance- oder Sicherheitsgründen (veraltet) in ein spezielles VLAN zu leiten.

# VLAN-Konfiguration



## Erstellen der Trunkverbindung (letzter Port). Kontrolle mittels CDP

### Trunk einschalten

Switch\_Etage01

SWITCH0\_Etage1(config)#int Gig0/1

SWITCH0\_Etage1(config-if)#switchport mode trunk

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1, changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1, changed state to up

SWITCH0\_Etage1(config-if)#no shut

SWITCH0\_Etage1(config-if)#exit

Switch1\_Etage2

Switch1\_Etage2(config)#int Gig0/1

Switch1\_Etage2(config-if)#switchport mode t

Switch1\_Etage2(config-if)#no shut

Switch1\_Etage2(config-if)#ex

## Konfiguration der VTP Clients & Server und erstellen der Domäne IFDOM

### Konfiguration von Switch0 als Server

SWITCH0\_Etage1(config)#vtp mode server

Device mode already VTP SERVER.

SWITCH0\_Etage1(config)#vtp version 2

SWITCH0\_Etage1(config)#vtp domain IFDOM

Changing VTP domain name from NULL to IFDOM

SWITCH0\_Etage1(config)#vtp password IFDOM

Setting device VLAN database password to IFDOM

### Konfiguration von Switch1 als Client

SWITCH1\_ETAGE2(config)#vtp mode client

Setting device to VTP CLIENT mode.

SWITCH1\_ETAGE2(config)#vtp domain IFDOM

Domain name already set to IFDOM.

SWITCH1\_ETAGE2(config)#vtp password IFDOM

Setting device VLAN database password to IFDOM

## Status anzeigen

### Switch0

SWITCH0\_Etage1#show vtp st

VTP Version : 2

Configuration Revision : 0

Maximum VLANs supported locally : 255

Number of existing VLANs : 5

VTP Operating Mode : Server

VTP Domain Name : IFDOM

VTP Pruning Mode : Disabled

VTP V2 Mode : Enabled

VTP Traps Generation : Disabled

MD5 digest : 0xD0 0x6B 0x11 0x1C 0x74 0x6C 0x61 0x33

Configuration last modified by 0.0.0.0 at 3-1-93 00:07:47

Local updater ID is 0.0.0.0 (no valid interface found)

### Switch1

SWITCH1\_ETAGE2#show vtp st

VTP Version : 2

Configuration Revision : 0

Maximum VLANs supported locally : 255

Number of existing VLANs : 5

VTP Operating Mode : Client

VTP Domain Name : IFDOM

VTP Pruning Mode : Disabled

VTP V2 Mode : Enabled

VTP Traps Generation : Disabled

MD5 digest : 0xD0 0x6B 0x11 0x1C 0x74 0x6C 0x61 0x33

Configuration last modified by 0.0.0.0 at 3-1-93 00:07:47

## Erstellen der VLANs

Derzeit ist die Datenbank an VLANs noch leer.

SWITCH0\_Etage1#vlan database

% Warning: It is recommended to configure VLAN from config mode,

as VLAN database mode is being deprecated. Please consult user

documentation for configuring VTP/VLAN in config mode.

### Verkauf-VLAN erstellen

SWITCH0\_Etage1(vlan)#vlan 2 name Verkauf

VLAN 2 added:

Name: Verkauf

### Einkaufs-VLAN erstellen

SWITCH0\_Etage1(vlan)#vlan 3 name Entwicklung

VLAN 3 added:

Name: Entwicklung

SWITCH0\_Etage1(vlan)#exit

APPLY completed.

Exiting....

## Zuweisen der Ports

1-3 zu Verkauf, 4-6 zu Entwicklung.

### Switch0

Verkaufs-VLAN:

SWITCH0\_Etage1(config)#int range fa0/1-3

SWITCH0\_Etage1(config-if-range)#switchport mode access

SWITCH0\_Etage1(config-if-range)#switchport access vlan 2

SWITCH0\_Etage1(config-if-range)#no shut

SWITCH0\_Etage1(config-if-range)#exit

Entwicklungs-VLAN:

SWITCH0\_Etage1(config)#int range fa0/4-6

SWITCH0\_Etage1(config-if-range)#switchport mode access

SWITCH0\_Etage1(config-if-range)#switchport access vlan 3

SWITCH0\_Etage1(config-if-range)#no shut

SWITCH0\_Etage1(config-if-range)#exit

### Switch1

Verkaufs-VLAN:

SWITCH1\_ETAGE2(config)#int range fa0/1-3

SWITCH1\_ETAGE2(config-if-range)#switchport mode access

SWITCH1\_ETAGE2(config-if-range)#switchport access vlan 2

SWITCH1\_ETAGE2(config-if-range)#no shut

SWITCH1\_ETAGE2(config-if-range)#exit

Entwicklungs-VLAN:

SWITCH1\_ETAGE2(config)#int range fa0/4-6

SWITCH1\_ETAGE2(config-if-range)#switchport mode access

SWITCH1\_ETAGE2(config-if-range)#switchport access vlan 3

SWITCH1\_ETAGE2(config-if-range)#no shut

SWITCH1\_ETAGE2(config-if-range)#exit

## Anzeige und Analyse der Konfiguration

### Switch0\_Etage1

SWITCH0\_Etage1#show vtp st

VTP Version : 2

Configuration Revision : 3

Maximum VLANs supported locally : 255

Number of existing VLANs : 7

VTP Operating Mode : Server

VTP Domain Name : IFDOM

VTP Pruning Mode : Disabled

VTP V2 Mode : Enabled

VTP Traps Generation : Disabled

MD5 digest : 0xF6 0xAF 0x8D 0x79 0xBD 0xEE 0xE5 0x72

Configuration last modified by 0.0.0.0 at 3-1-93 00:19:36

Local updater ID is 0.0.0.0 (no valid interface found)

### Switch1\_Etage2

SWITCH1\_ETAGE2#show vtp st

VTP Version : 2

Configuration Revision : 3

Maximum VLANs supported locally : 255

Number of existing VLANs : 7

VTP Operating Mode : Client

VTP Domain Name : IFDOM

VTP Pruning Mode : Disabled

VTP V2 Mode : Enabled

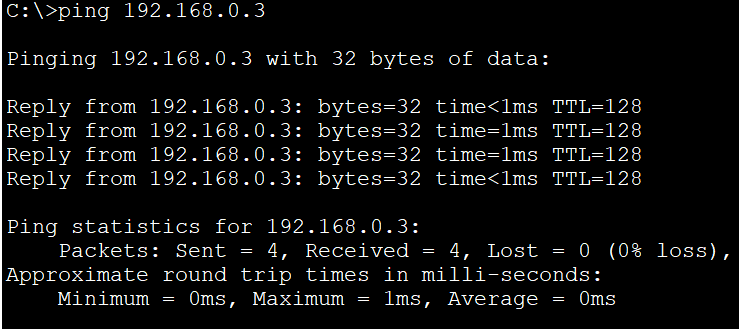
VTP Traps Generation : Disabled

MD5 digest : 0xF6 0xAF 0x8D 0x79 0xBD 0xEE 0xE5 0x72

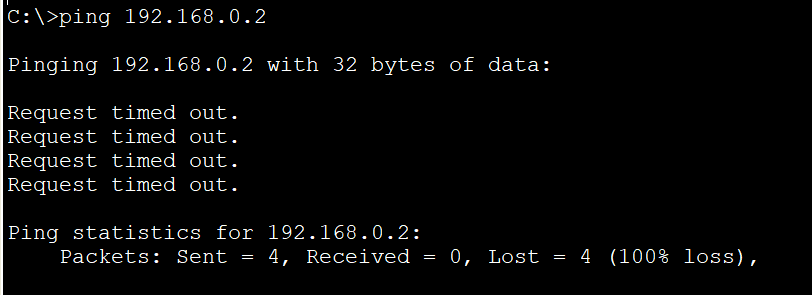
Configuration last modified by 0.0.0.0 at 3-1-93 00:19:36

## Ping-Test

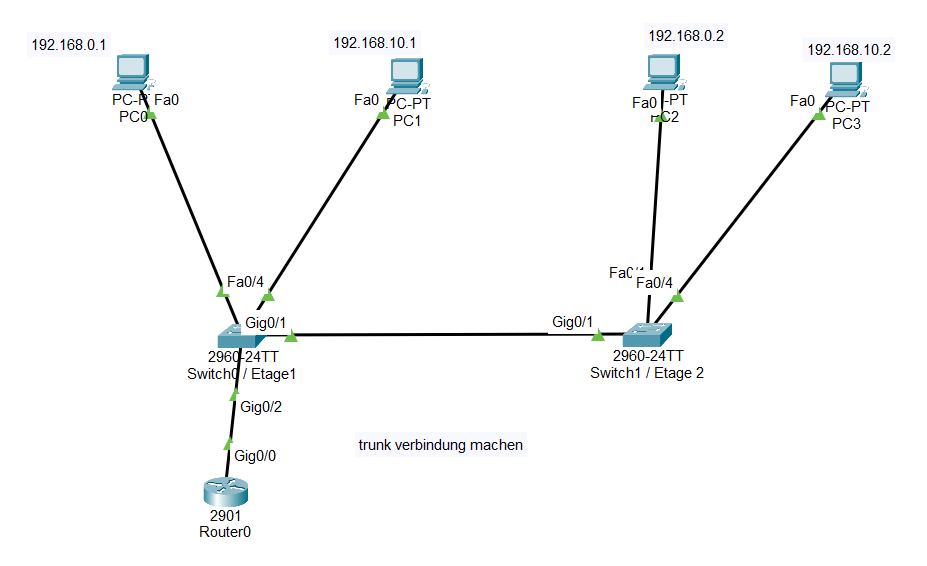
Von Verkaufs-VLAN-PC zu anderem PC in selbem VLAN:



Von Verkaufs-VLAN-PC zu einem PC in Entwicklungs-VLAN:



# Inter-VLAN Routing



## Konfiguration:

### Für VLAN 10

Enter configuration commands, one per line. End with CNTL/Z.

Router(config)#int g0/0

Router(config-if)#no shut

Router(config-if)#exit

Router(config)#int g0/0.2

Router(config-subif)#encapsulation dot1Q 10

Router(config-subif)#ip address 192.168.0.254 255.255.255.0

Router(config-subif)#no shut

Router(config-subif)#exit

### FÜR VLAN 20:

Router(config)#int g0/0.3

Router(config-subif)#

%LINK-5-CHANGED: Interface GigabitEthernet0/0.3, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0.3, changed state to up

Router(config-subif)#encapsulation dot1Q 20

Router(config-subif)#ip address 192.168.10.254 255.255.255.0

Router(config-subif)#no shut

Router(config-subif)#exit

## Ping Test

Hier wird von 192.168.0.1 zu 192.168.10.2 gepingt.

Ping von PC0 zu PC3:

C:\>ping 192.168.10.2

Pinging 192.168.10.2 with 32 bytes of data:

Reply from 192.168.10.2: bytes=32 time<1ms TTL=127

Reply from 192.168.10.2: bytes=32 time=1ms TTL=127

Reply from 192.168.10.2: bytes=32 time<1ms TTL=127

Reply from 192.168.10.2: bytes=32 time=1ms TTL=127

Ping statistics for 192.168.10.2:

Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),

Approximate round trip times in milli-seconds:

Minimum = 0ms, Maximum = 1ms, Average = 0ms

Ping von PC3 zu PC0:

C:\>ping 192.168.0.1

Pinging 192.168.0.1 with 32 bytes of data:

Reply from 192.168.0.1: bytes=32 time<1ms TTL=127

Reply from 192.168.0.1: bytes=32 time<1ms TTL=127

Reply from 192.168.0.1: bytes=32 time<1ms TTL=127

Reply from 192.168.0.1: bytes=32 time<1ms TTL=127

Ping statistics for 192.168.0.1:

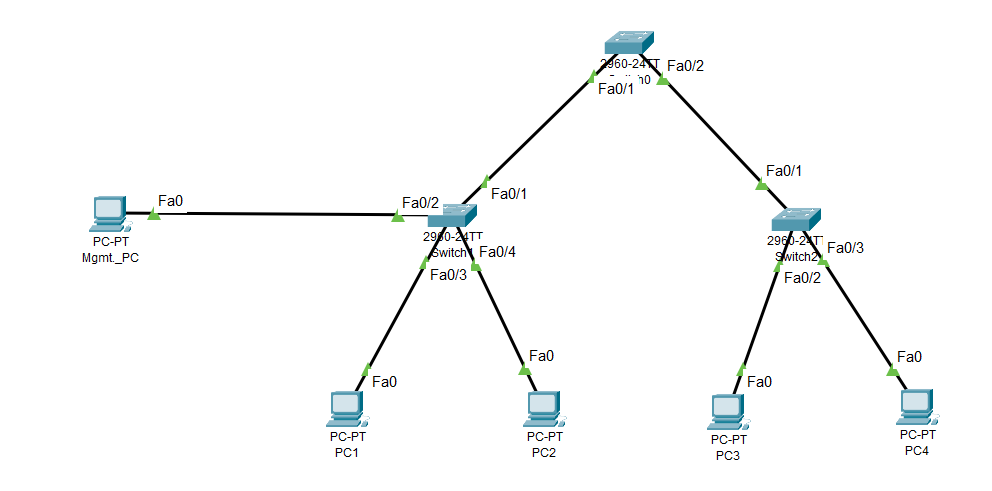
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),

Approximate round trip times in milli-seconds:

Minimum = 0ms, Maximum = 0ms, Average = 0ms

# Management\_Fernwartung

Netzwerk-Aufbau: Oberster Switch ist Switch0, der Core-Switch.



## VLAN Konfiguration an allen 3 Switches

### Switch0 – Core-Switch

SWITCH0(config)#int vlan1

SWITCH0(config-if)#ip address 192.168.0.200 255.255.255.0

SWITCH0(config-if)#no shut

SWITCH0(config-if)#

%LINK-5-CHANGED: Interface Vlan1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to up

### Switch1

SWITCH1(config)#int vlan1

SWITCH1(config-if)#ip a 192.168.0.201 255.255.255.0

SWITCH1(config-if)#no shut

SWITCH1(config-if)#

%LINK-5-CHANGED: Interface Vlan1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to up

### Switch2

SWITCH2(config)#int vlan1

SWITCH2(config-if)#ip a 192.168.0.202 255.255.255.0

SWITCH2(config-if)#no shut

%LINK-5-CHANGED: Interface Vlan1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to up

## SSH Zugang einrichten

Es soll ein SSH Zugang mit folgenden Daten eingerichtet werden:

User: cisco

Passwort: ciscossh

### Switch0

SWITCH0(config)#username cisco password ciscossh

SWITCH0(config)#ip domain-name nvs.lan

SWITCH0(config)#crypto key generate rsa

The name for the keys will be: SWITCH0.nvs.lan

Choose the size of the key modulus in the range of 360 to 2048 for your

General Purpose Keys. Choosing a key modulus greater than 512 may take

a few minutes.

How many bits in the modulus [512]: 1024

% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]

\*Mar 1 0:12:38.228: %SSH-5-ENABLED: SSH 1.99 has been enabled

SWITCH0(config)#line vty 04

SWITCH0(config-line)#login local

SWITCH0(config-line)#transport input ssh

SWITCH0(config-line)#exit

SWITCH0(config)#ip ssh version 2

SWITCH0(config)#service password-encryption

### Switch1

SWITCH1(config)#username cisco password ciscossh

SWITCH1(config)#ip domain-name nvs.lan

SWITCH1(config)#crypto key generate rsa

The name for the keys will be: SWITCH1.nvs.lan

Choose the size of the key modulus in the range of 360 to 2048 for your

General Purpose Keys. Choosing a key modulus greater than 512 may take

a few minutes.

How many bits in the modulus [512]: 1024

% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]

SWITCH1(config)#line vty 04

\*Mar 1 0:17:3.937: %SSH-5-ENABLED: SSH 1.99 has been enabled

SWITCH1(config-line)#login local

SWITCH1(config-line)#transport input ssh

SWITCH1(config-line)#exit

SWITCH1(config)#ip ssh version 2

SWITCH1(config)#service password-encryption

### Switch2

SWITCH2(config)#username cisco password ciscossh

SWITCH2(config)#ip domain-n

SWITCH2(config)#ip domain-name nvs.lan

SWITCH2(config)#crypto key generate rsa

The name for the keys will be: SWITCH2.nvs.lan

Choose the size of the key modulus in the range of 360 to 2048 for your

General Purpose Keys. Choosing a key modulus greater than 512 may take

a few minutes.

How many bits in the modulus [512]: 1024

% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]

SWITCH2(config)#line vty 0 4

\*Mar 1 0:20:15.326: %SSH-5-ENABLED: SSH 1.99 has been enabled

SWITCH2(config-line)#transport input ssh

SWITCH2(config-line)#login local

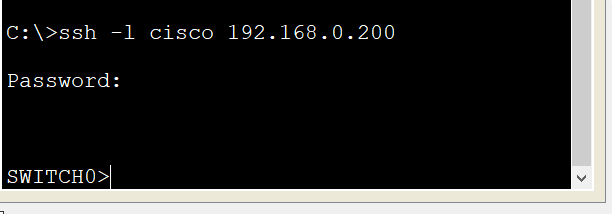
SWITCH2(config-line)#exit

SWITCH2(config)#ip ssh version 2

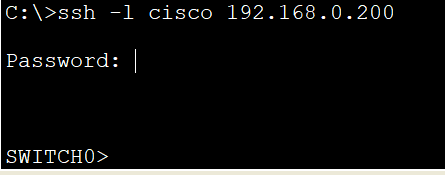
SWITCH2(config)#service password-encryption

## Testen Sie den Zugriff. Von welchen PC’s können sie zugreifen? Ist das zufriedenstellen?

Management-PC:



PC1:



## Konfigurieren Sie den Coreswitch als VTP Server (Domäne NVSDom)

SWITCH0(config)#vtp mode server

Device mode already VTP SERVER.

SWITCH0(config)#vtp version 2

SWITCH0(config)#vtp domain NVSDom

Changing VTP domain name from NULL to NVSDom

SWITCH0(config)#vtp password NVSDom

Setting device VLAN database password to NVSDom

## Konfigurieren der Switches und Trunk-Verbindungen

### Core-Switch

SWITCH0(config)#int fa0/1

SWITCH0(config-if)#switchport mode trunk

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up

SWITCH0(config-if)#no shut

SWITCH0(config)#int fa0/2

SWITCH0(config-if)#switchport mode trunk

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/2, changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/2, changed state to up

SWITCH0(config-if)#no shut

### Switch 1

SWITCH1(config)#int fa0/1

SWITCH1(config-if)#switchport mode trunk

SWITCH1(config-if)#no shut

SWITCH1(config-if)#end

### Switch 2

SWITCH2(config)#int fa0/1

SWITCH2(config-if)#switchport mode trunk

SWITCH2(config-if)#no shut

SWITCH2(config-if)#exit

## VLAN 10 als Client-VLAN einrichten

### Am Core-Switch

SWITCH0#vlan database

% Warning: It is recommended to configure VLAN from config mode,

as VLAN database mode is being deprecated. Please consult user

documentation for configuring VTP/VLAN in config mode.

SWITCH0(vlan)#vlan 10 name clientvlan

VLAN 10 added:

Name: clientvlan

### Switch 1

SWITCH1(config)#vtp mode client

Setting device to VTP CLIENT mode.

SWITCH1(config)#vtp password NVSDom

Setting device VLAN database password to NVSDom

### Switch 2

SWITCH2(config)#vtp mode client

Setting device to VTP CLIENT mode.

SWITCH2(config)#vtp password NVSDom

Setting device VLAN database password to NVSDom

## Ports auf das VLAN setzen

### Switch1

SWITCH1(config)#int range fa0/3-24

SWITCH1(config-if-range)#switchport mode access

SWITCH1(config-if-range)#switchport access vlan 10

SWITCH1(config-if-range)#no shut

SWITCH1(config-if-range)#exit

### Switch 2

SWITCH2(config)#int range fa0/2-24

SWITCH2(config-if-range)#switchport mode access

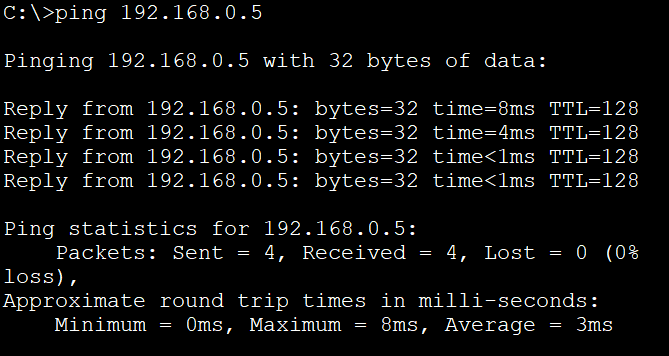
SWITCH2(config-if-range)#switchport access vlan 10

SWITCH2(config-if-range)#no shut

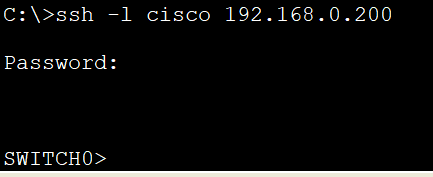
SWITCH2(config-if-range)#exit

SWITCH2(config)#

Ping Test von PC1 zu PC4:



## SSH Zugriff testen

**Von Management PC:**

**Von PC1:**

