Abteilung für INFORMATIK

HTL ST. PÖLTEN

Titel: Labor04 – Spanning Tree & SSH

Klasse: 4BHIF

Name: Haiden

Gruppe: 01

Aufgabe: 01.12.2020 Abgabe: 15.12.2020

Inhaltsverzeichnis

1 Theorie-Teil ... 1

1.1 STP ... 1

1.2 Wie wird die Root Bridge bestimmt / Das erste Ereignis ... 1

1.3 Die Bildung des Spanning Trees ... 1

1.4 Zustände eines Switch-Ports ... 1

1.5 Weiterentwicklungen (RTSP, MSTP) ... 2

1.6 BDPUs ... 2

1.7 Broadcast-Storm ... 2

1.7.1 Ursachen: ... 2

2 Fragen ... 3

2.1 Beantworten Sie zuerst theoretisch folgende Fragen: ... 3

2.2 Welcher Switch wird die Rootbridge? Warum? ... 3

2.3 Welche Ports werden Root-Port? Warum. ... 4

2.4 Wo ist der Non-Designated/Designated Ports? Wie kommt diese Entscheidung zustande? ... 4

2.5 Ändern Sie die Konfiguration damit ein anderer SwitchRootBridge wird. Wie verläuft diese Änderung ... 5

2.6 Spanning Tree deaktivieren? Was passiert? ... 6

2.6.1 Zum Aktivieren: ... 6

3 MAC-Table & Clients ... 8

3.1 Verbinden Sie Clients mit dem Switches ... 8

3.2 Wie können Sie die MAC-Table anzeigen? ... 8

3.3 Wie viele Einträge sind möglich? ... 9

3.4 Wie lange ist die Holdown-Time? Kann diese verändert werden? ... 9

4 SSH & Webinterface ... 9

4.1 SSH Zugang einrichten ... 9

4.2 Webinterface? ... 11

1 Theorie-Teil

1.1 STP

Quelle: https://www.ip-insider.de/was-ist-stp-spanning-tree-protocol-a-664041/

Das Spanning Tree Protocol ist gängiges und weitläufiges Protokoll, welches in Ethernet-Topologien bei denen mehrere, parallele Switches eingesetzt werden, vorkommt. Es soll durch das Bestimmen einer Root Bridge und entsprechenden Maßnahmen sicherstellen, dass Effekte wie Schleifen und Broadcaststürme nicht vorkommen. Es funktioniert in beliebig großen Netzwerk-Strukturen und erzeugt eine baumartige Topologie mit eindeutigen Verbindungspfaden, bis hinauf zur Root-Bridge, oder der Wurzel, analog zu einem Baum.

Es wurde 1990 in der IEEE-Norm 802.1D standardisiert. Durch das Herstellen eindeutiger Pfade in geswitchten Umgebungen soll sichergestellt werden, dass keine Schleifen auftreten. Auch Netzwerkphänomene wie Broadcast-Stürme sollen durch STP verhindert werden.

Das Ergebnis eines erfolgreichen Zusammenspiels der Switches ist eine baumartige Topologie. Sie enthält keine doppelten / mehrfachen Verbindungen zu Quelle und Ziel, sondern geht stetig eine Stufe nach oben, bis zur Root-Bridge. STP stellt sicher, dass jeder Punkt ideal erreichbar ist und arrangiert so die Switches. Fällt ein Switch aus, so merkt STP das und stellt durch ein erneutes Organisieren einer Baumtopologie sicher, dass Daten effizient und sicher fließen.

1.2 Wie wird die Root Bridge bestimmt / Das erste Ereignis

Das erste Ereignis im Leben einer STP Topolgie beginnt damit, eine Root Bridge zu ernennen. Sie ist die Wurzel der Baumtopologie und ist das bestimmende Element in der Topologie. Sie wird nach einem definierten Verfahren bestimmt. Über Multicast-Nachrichten machen sich die Switches über die sogenannte Bridge-ID, eine 8 Byte lange Information, welche aus Priorität, System-ID und Mac-Adresse besteht, klar, wer wer ist. Der Switch, welcher die niedrigste Priorität aufweist, zur Root Bridge und wird zur Wurzel der Topologie. Gibt es in einer geswitchten Umgebung jedoch zwei oder mehr Switches, welche dieselbe Priorität aufweisen, dann entscheidet die MAC-Adresse.

1.3 Die Bildung des Spanning Trees

Ist die Root Bridge einmal auserwählt, kann man damit beginnen, die baumähnliche Topologie aufzubauen. Von der Root Bridge werden die Pfadkosten und Wege bestimmt, wie andere Switches zu erreichen sind. Gibt es mehrere Pfade, werden solche mit den meisten Pfadkosten deaktiviert. (NDP.)

Pfadkosten setzen sich aus Bandbreite der Links (bei Gigabit: 4, FE: 19) und der Anzahl überwindender Knoten zusammen. Der IEEE-Standard für STP definiert die Pfadkosten, sie können jedoch auch manuell gesetzt werden.

Gibt es von einem Switch im Aufbau keine Hello-Pakete mehr, so geht STP von einem Ausfall der Strecke oder eines Switches aus und reorganisiert die Baumstruktur. Wird gerade reorganisiert, können Switches keine anderen Pakete weiterleiten, erst wenn es wieder reorganisiert ist werden andere Pakete weitergeschickt.

1.4 Zustände eines Switch-Ports

- Forwarding: Leiten Frames weiter, empfangen BDPUs und lernen neue Adressen. Sie sind komplett aktiv.
- Blocking: Verwerfen Frames, lernen keine Adressen, empfangen aber wie Forwarding BDPUs.

Nach der Aktivierung von STP durchlaufen die Ports nacheinander die Zustände

- Blocking
- Listening
- Learning
- Forwarding

Timer und BDPUs sorgen für eine konfliktfreie Übergang der einzelnen Stücke und bestimmen die Konvergenzzeit, die Zeit die benötigt wird um einen STP zu berechnen oder neu zu bestimmen.

1.5 Weiterentwicklungen (RTSP, MSTP)

STP hat lange Konvergenzzeiten. Daher wurden RSTP und MSTP ins Leben gerufen und standardisiert. Im Gegensatz zu STP arbeitet RSTP mit der Topologie weiter, während sich eine neue aufbaut. So kann man lange Ausfallszeiten vermeiden. MSTP ist eine Weiterentwicklung von RSTP und ermöglicht das Bilden von unabhängigen STP-Instanzen für VLANs. In einem Netzwerk können dank MSTP dann Mehrere Baumtopologien für mehrere VLANs exisitieren.

1.6 BDPUs

https://www.itwissen.info/BPDU-bridge-protocol-data-unit.html

Die Bridge Protocol Data Unit (BDPUs) ist eine Dateneinheit für das Spanning-Tree Protokoll. Sie dient Switches und Brücken, die das STP Protokoll nutzen, zum Austausch von Management- und Steuerinformationen zwischen den Switches & Brücken eines Netzwerkes. Es besteht aus mehreren Datenfeldern:

- Destination-Adresse: Enthält die Zieladresse der Root-Bridge aus Sicht der sendenden Brücke.
- Source-Adresse: Die Adresse des Absenders bzw. der sendenden Brücke. Enthält Adresse und Portbezeichnung.
- Längenfeld: Gibt die Länge des BDPUs Paketes an.
- DSAP (Data Service Access Point), SSAP (Source Service Access Point): Individuelle Zell- und Quelladressen, oder zusammengefasste Gruppenadresse einer MAC.
- Konfig.-Nachricht: Konfigurationsnachricht mit wichtigen Infos über entsprechenden Streckenabschnitt

BDPUs werden alle 2 Sekunden versendet. Empfangende Brücken nutzen sie, um Routen zu optimieren. Sie dienen der Schleifenunterdrückung im Netzwerk und Verbesserung des Netzwerkverkehrs.

1.7 Broadcast-Storm

https://de.wikipedia.org/wiki/Broadcast-Sturm

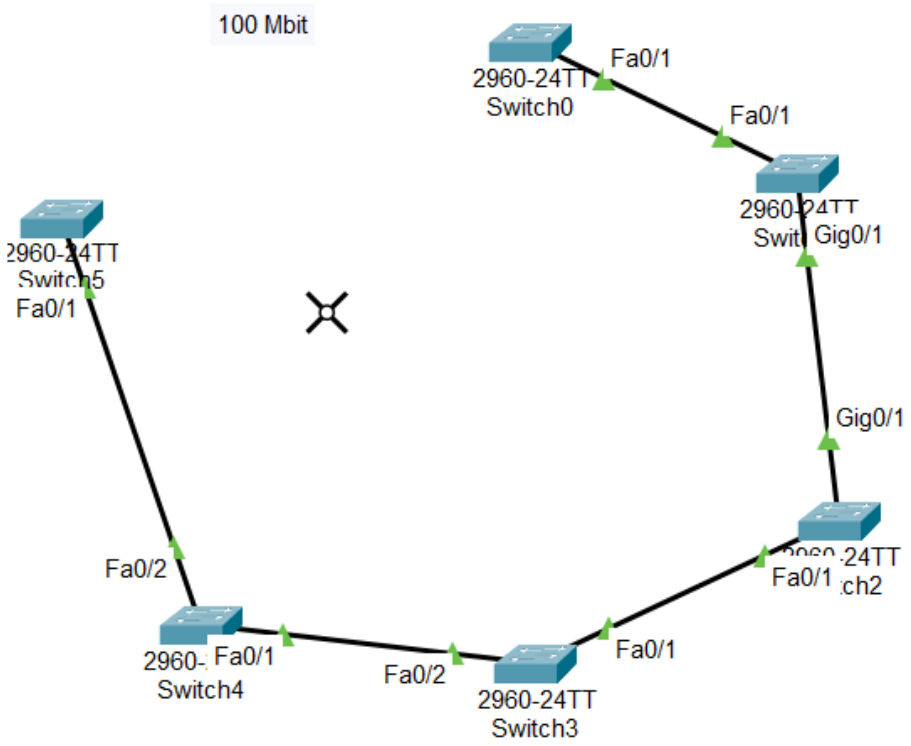
Broadcast Storms sind eine starke Anhäufung von Broadcast- und Multicast Verkehr im Netzwerk. Im Endstadium eines solchen Sturms sind neue Verbindungen nicht mehr möglich, bereits bestehende Verbindungen werden möglicherweise unterbrochen. In großen Domänen kann sich die Antwortzeit durch einen Schneeballeffekt drastisch erhöhen.

1.7.1 Ursachen:

Die häufigste Ursache ist eine redundante Verkabelung mit zwei oder mehr Uplinks zwischen zwei Switches. Hier werden Broadcast und Multicast Anfragen auf alle Ports weitergeleitet, außer woher der eigentliche Datenverkehr kam. Dadurch wird eine Schleife erzeugt, und die Broadcasts werden an andere Switches weitergeleitet. Solche Stürme können auch durch DoS-Attacken ausgeführt werden.

2 Fragen

2.1 Beantworten Sie zuerst theoretisch folgende Fragen:



2.2 Welcher Switch wird die Rootbridge? Warum?

Der Switch mit der niedrigsten Bridge-ID / Priorität wird die Root-Bridge im Netzwerk. Gibt es allerdings Switches mit der gleichen Bridge-ID / Priorität, so wird der Switch mit der niedrigsten MAC-Adresse die Root-Bridge.

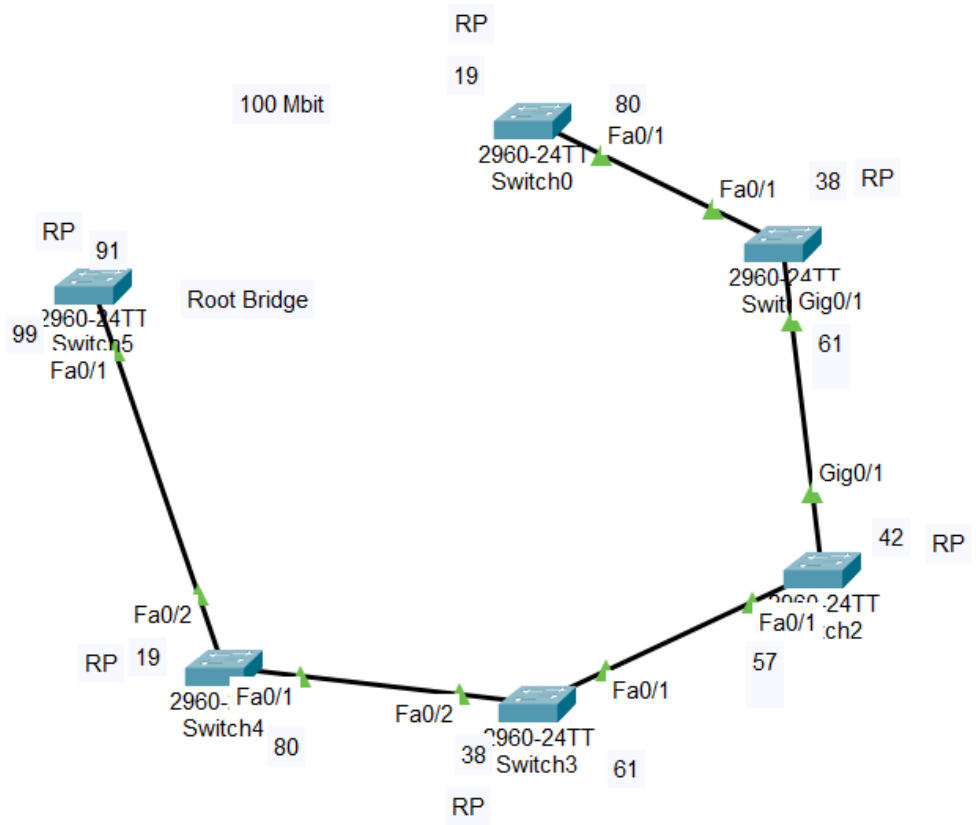
Meine Vermutung ist, dass der Switch5 (links in der Mitte) zur Root-Bridge wird.

```
SWITCH5#show sp

VLAN0001

Spanning tree enabled protocol ieee

Root ID Priority 32769

Address 000B.BE61.BC86

This bridge is the root

Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
```

```
Bridge ID Priority 32769 (priority 32768 sys-id-ext 1)
Address 000B.BE61.BC86
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
Aging Time 20
Interface Role Sts Cost Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------
---------
Fa0/2 Desg FWD 19 128.2 P2p
Fa0/1 Desg FWD 19 128.1 P2p
```

2.3 Welche Ports werden Root-Port? Warum.

Der Port beim Switch mit den niedrigsten Kosten zur Root Bridge wird zum Root Port. Ein Switch kann nur einen Root Port haben.

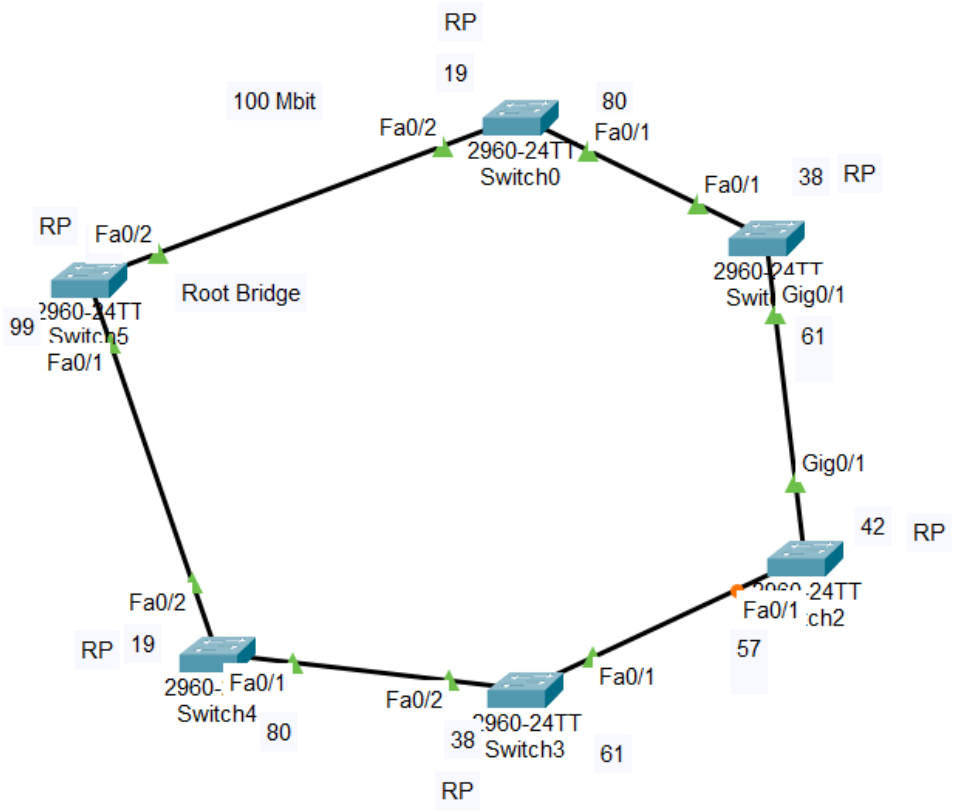


2.4 Wo ist der Non-Designated/Designated Ports? Wie kommt diese Entscheidung zustande?

Der Port, welcher die geringsten Kosten zu einem LAN-Segment hat, wird zum Designated Port. Es kann davon mehrere an einem Switch geben. Ein Designated Port kann nie ein Root Port sein.

Der Non-Designated Port ist am Ende eines Designated Ports. Befindet sich dort kein Root Port, so wird er zum Non-Designated Port. NDP sind dazu da, Switching Loops auf Layer 2 im OSI-Modell zu vermeiden. Sie blockieren den Datentransfer und lassen so keine Pakete durch, damit kein Loop entstehen kann.

Im Modell von oben wird Fa0/1 an Switch 2 ein NDP, da das andere Ende nicht an einen Root Port angeschlossen ist und es ist die höheren Kosten hat.



2.5 Ändern Sie die Konfiguration damit ein anderer SwitchRootBridge wird. Wie verläuft diese Änderung

Switch5 ist derzeit die Root Bridge. Um jetzt z.B. Switch0 zur Root-Bridge machen zu können, muss man seine Priorität im Global Conf. Mode ändern.

Dazu benutzt man folgendes Kommando-Schema:

```
spanning-tree vlan <VLAN_NO> priority <PRIORITY_NO>
```

Beispiel, an Switch0:

```
SWITCH0(config)#spanning-tree vlan 1 priority 0
SWITCH0(config)#exit
SWITCH0#show sp
VLAN0001
Spanning tree enabled protocol ieee
Root ID Priority 1
Address 00D0.97D2.D7DE
This bridge is the root
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Bridge ID Priority 1 (priority 0 sys-id-ext 1)
Address 00D0.97D2.D7DE
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
Aging Time 20
Interface Role Sts Cost Prio.Nbr Type
---------------- ---- --- --------- -------- ----------------------
---------
Fa0/2 Desg FWD 19 128.2 P2p
Fa0/1 Desg FWD 19 128.1 P2p
```

2.6 Spanning Tree deaktivieren? Was passiert?

Mit

```
no spanning-tree vlan <VLAN_NO>
```

kann man Spanning Tree für ein bestimmtes VLAN abschalten. Zuerst wird nichts passieren, allerdings, wenn man später einen Client connected, entwickelt sich ein „Broadcast Sturm“. Die Switches werden mit Broadcasts überfüllt und da sie sich nicht untereinander koordinieren können, tritt das Loop Problem auf der Layer 2 OSI Schicht in Kraft.

```
SWITCH0(config)#no spanning-tree vlan 1
SWITCH0(config)#exit
SWITCH0#show sp
No spanning tree instance exists.
```

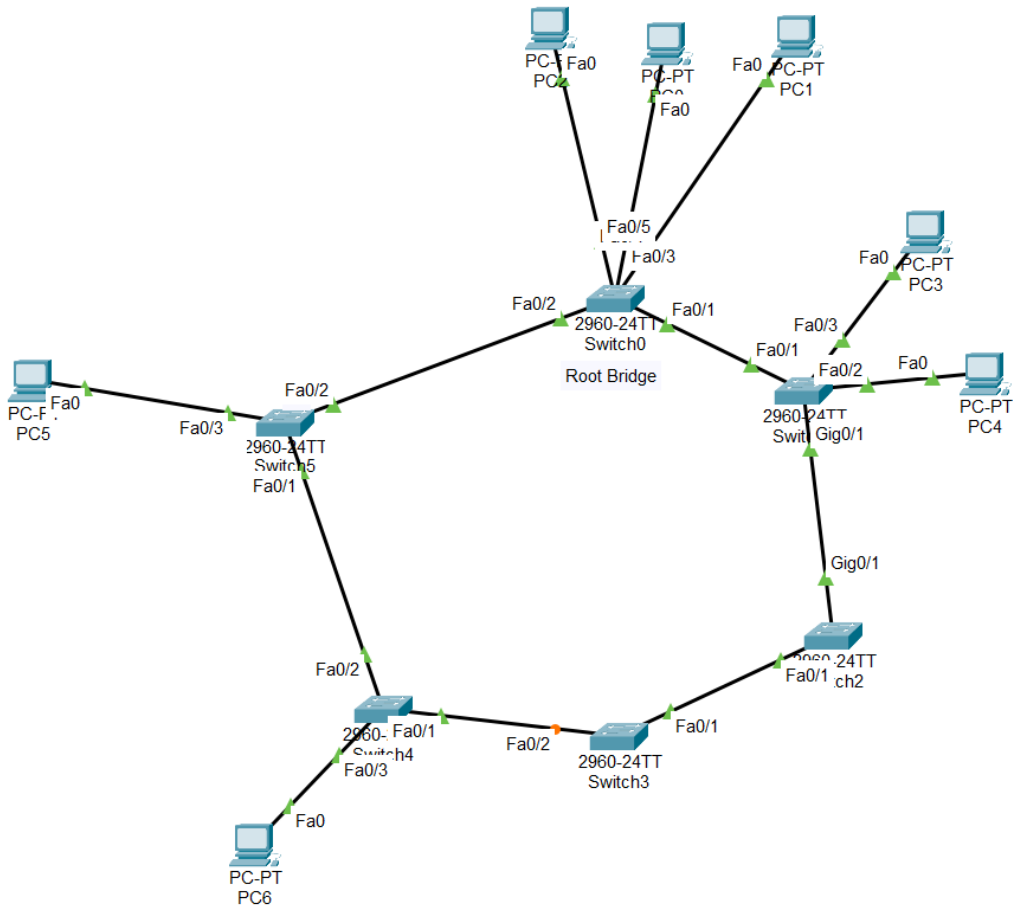
2.6.1 Zum Aktivieren:

Zum Aktivieren in den Global Conf Mode gehen und dort `spanning-tree vlan <VLAN_NO>` eingeben.

```
SWITCH0(config)#spanning-tree vlan 1
SWITCH0(config)#exit
SWITCH0#show sp
VLAN0001
Spanning tree enabled protocol ieee
Root ID Priority 1
Address 00D0.97D2.D7DE
This bridge is the root
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
Bridge ID Priority 1 (priority 0 sys-id-ext 1)
Address 00D0.97D2.D7DE
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
Aging Time 20
Interface Role Sts Cost Prio.Nbr Type
---------------- ---- --- --------- -------- ----------------------
---------
Fa0/3 Desg FWD 19 128.3 P2p
Fa0/2 Desg FWD 19 128.2 P2p
Fa0/1 Desg FWD 19 128.1 P2p
Fa0/4 Desg FWD 19 128.4 P2p
Fa0/5 Desg FWD 19 128.5 P2p
```

3 MAC-Table & Clients

3.1 Verbinden Sie Clients mit dem Switches



3.2 Wie können Sie die MAC-Table anzeigen?

Mit `show mac address-table` kann man sich die Tabelle anzeigen lassen.

```
SWITCH0#show mac-address-table
Mac Address Table
-------------------------------------------
Vlan Mac Address Type Ports
---- ----------- -------- -----
1 0001.6386.e802 DYNAMIC Fa0/2
1 00e0.8f30.9301 DYNAMIC Fa0/1
```

3.3 Wie viele Einträge sind möglich?

Um sich die Anzahl der maximal unterstützten Mac-Adressen Einträge anzusehen, kann man das Kommando show sdm prefer nutzen. Es zeigt die Grenzen für VLANs, IPs usw… an und gibt Auskunft darüber, wie viel der Switch unterstützt. Aus dem Output unten geht hervor, dass dieser Switch 8000 (8k, kurzgeschrieben) MAC-Adressen unterstützt. So unterstützt er auch 255 VLANs.

```
SWITCH0#show sdm prefer
The current template is "default" template.
The selected template optimizes the resources in
the switch to support this level of features for
0 routed interfaces and 255 VLANs.
number of unicast mac addresses: 8K
number of IPv4 IGMP groups: 256
number of IPv4/MAC qos aces: 128
number of IPv4/MAC security aces: 384
```

3.4 Wie lange ist die Holdown-Time? Kann diese verändert werden?

Die standardmäßigen Holdown-Time sind 180 Sekunden, direkt verändern kann man diese nicht. Die Holdtown Time wird durch das Advertisment Interval * 3 berechnet und so kann man nur den Multiplikator ändern.

4 SSH & Webinterface

4.1 SSH Zugang einrichten

Zuerst in den Global Configuration Mode wechseln. Wir nehmen hier als Beispiel wieder SWITCH0.

Hier in der Kommandozeile:

Ins entsprechende Interface wechseln, IP, Subnetzmaske vergeben. Dann das Interface starten und einen Domain-Namen vergeben.

```
SWITCH0(config)#interface vlan 1
SWITCH0(config-if)#ip address 192.168.0.1 255.255.255.0
SWITCH0(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
SWITCH0(config-if)#ip domain-name switch0_hai
```

Dann in den Global Configuration Mode zurück und dort RSA Crypto Keys generieren.

```
SWITCH0(config)#crypto key generate rsa

*Mar 2 1:32:38.769: RSA key size needs to be at least 768 bits for
ssh version 2

*Mar 2 1:32:38.769: %SSH-5-ENABLED: SSH 1.5 has been enabled

% You already have RSA keys defined named SWITCH0.switch0_hai .

% Do you really want to replace them? [yes/no]: yes

The name for the keys will be: SWITCH0.switch0_hai

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]
```

Danach muss man das Passwort und den Benutzernamen setzen.

```
SWITCH0(config)#username haiden password pass

*Mar 2 1:32:48.153: %SSH-5-ENABLED: SSH 1.99 has been enabled
```

Zuletzt noch einstellen, dass der Input auf SSH umgeleitet wird und dass man sich lokal einloggen darf.

```
SWITCH0(config)#line vty 0 15

SWITCH0(config-line)#transport input ssh

SWITCH0(config-line)#login local
```

Am PC:

```
C:\>ssh -l haiden 192.168.0.1

Password:

haiden>
```

4.2 Webinterface?

Da man beim Packet Tracer keine WebGUI aufrufen kann, hab ich hier beispielhaft einen Screenshot aus dem Internet eingefügt.