
Praktikum Rechnernetze

Protokoll zu Versuch 8 (Switching im LAN) von Gruppe 1

Jakob Waibel, Daniel Hiller, Elia Wüstner, Felix Pojtinger

2021-12-07

Inhaltsverzeichnis

1	Einführung	3
1.1	Mitwirken	3
1.2	Lizenz	3
2	Allgemeines	4
3	Switch Konfiguration	4
4	Analyse mit Wireshark	16
5	Konfigurationsdatei	19
6	Spanning-Tree-Verfahren	22
7	Port Mirroring und Port Security	29
8	VLANs	32
9	Sichern der Konfiguration	37

1 Einführung

1.1 Mitwirken

Diese Materialien basieren auf [Professor Kiefers “Praktikum Rechnernetze”-Vorlesung der HdM Stuttgart](#).

Sie haben einen Fehler gefunden oder haben einen Verbesserungsvorschlag? Bitte eröffnen Sie ein Issue auf GitHub (github.com/pojntfx/uni-netpractice-notes):



Abbildung 1: QR-Code zum Quelltext auf GitHub

Wenn ihnen die Materialien gefallen, würden wir uns über einen GitHub-Stern sehr freuen.

1.2 Lizenz

Dieses Dokument und der enthaltene Quelltext ist freie Kultur bzw. freie Software.



Abbildung 2: Badge der AGPL-3.0-Lizenz

Uni Network Practice Notes (c) 2021 Jakob Waibel, Daniel Hiller, Elia Wüstner, Felix Pojtinger

SPDX-License-Identifier: AGPL-3.0

2 Allgemeines

Mal ganz dumm gefragt: Wieso haben manche Switches als Layer-2-Koppelement eigentlich eine IP-Adresse?

TODO: Add answer

Ist ein Switch der eine IP-Adresse hat, automatisch ein Layer-3-Switch

TODO: Add answer

Was ist der Unterschied zwischen einem Layer-3-Switch und einem Router?

TODO: Add answer

3 Switch Konfiguration

Sie bekommen die Switche sozusagen „originalverpackt“. Um die Geräte initial zu konfigurieren, müssen Sie ein serielles Kabel (Console) an den PC anschließen und Putty oder MobaXterm (Console Serial: COMx, Speed: 9600; Console USB: COMx, Speed: 9600) starten

**Abbildung 3:** PuTTY setup

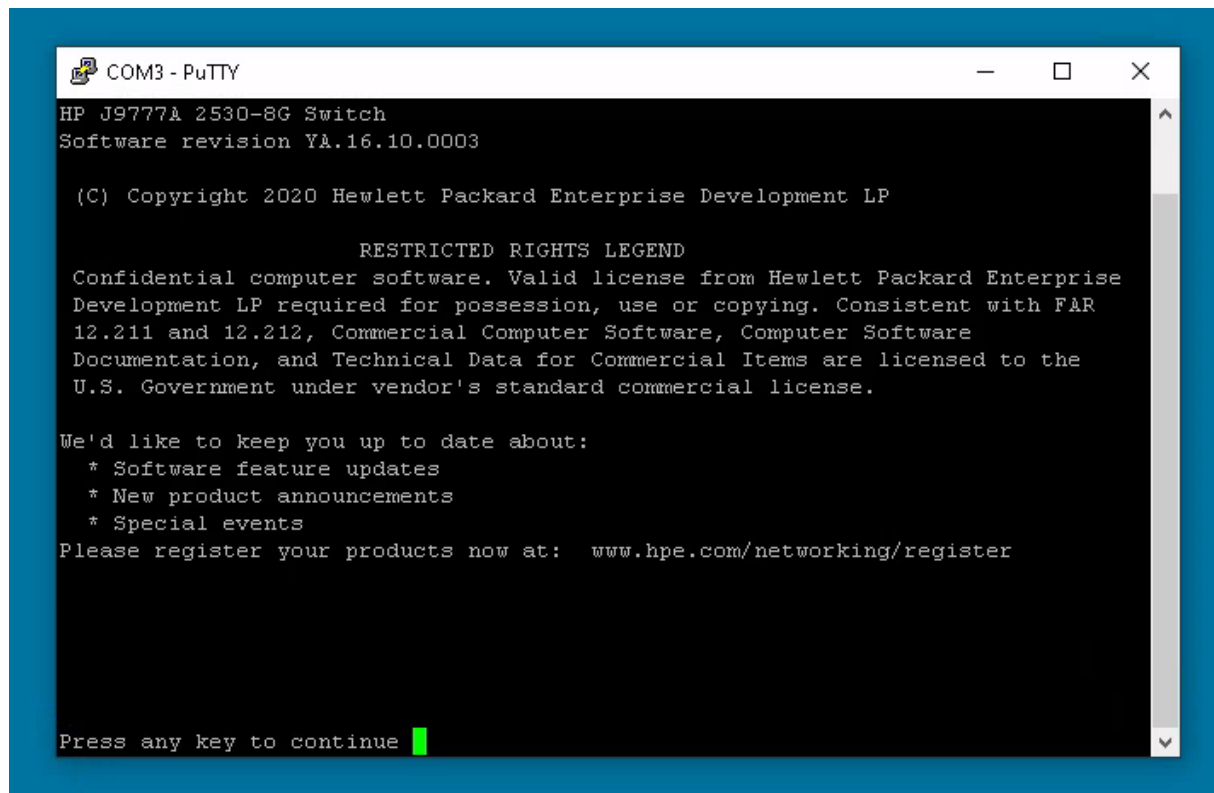


Abbildung 4: PuTTY logged in

Zur Sicherheit setzen Sie nach erfolgreicher Verbindung ihren Switch auf Werkszustand zurück. Das geht über die Console mit dem Befehl `erase all`. (Anm.: Da an dem Switch auch ihr PC mit RDP dranhängt, geht auch die RDP-Verbindung verloren. D.h. Sie müssen sich anschließend neu mit RDP auf ihrem PC anmelden)

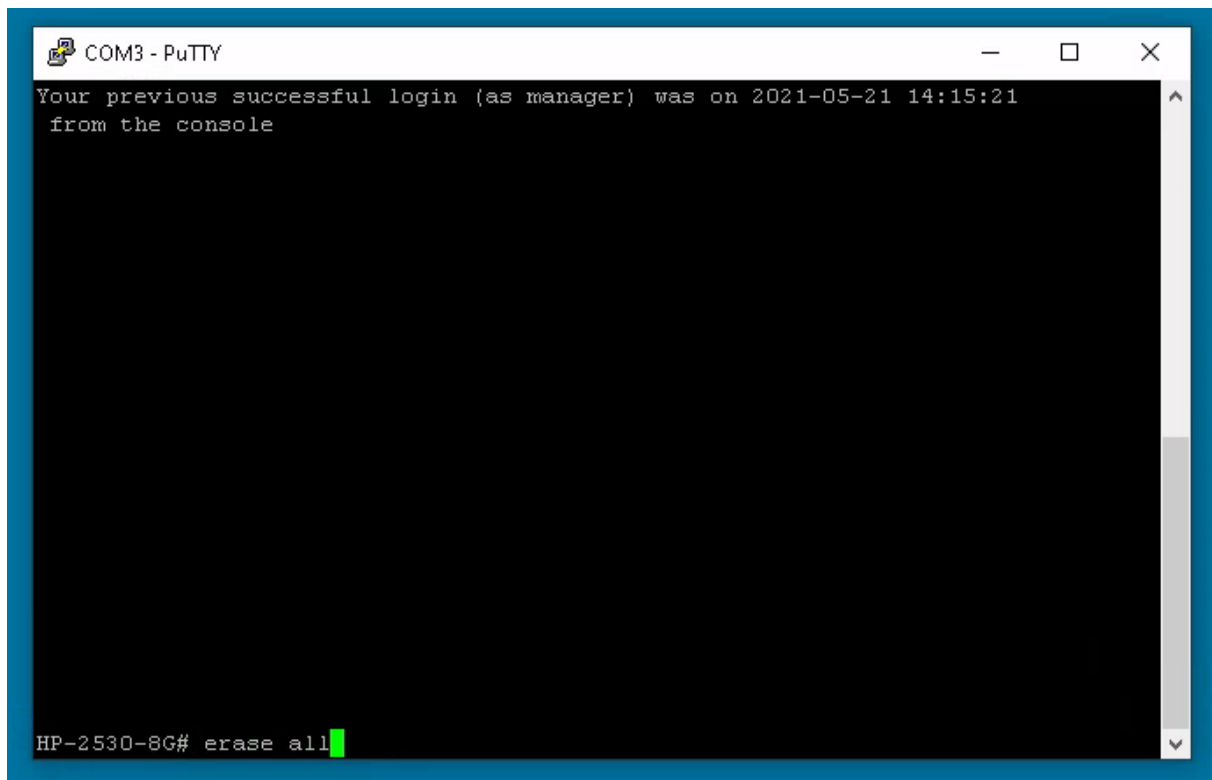
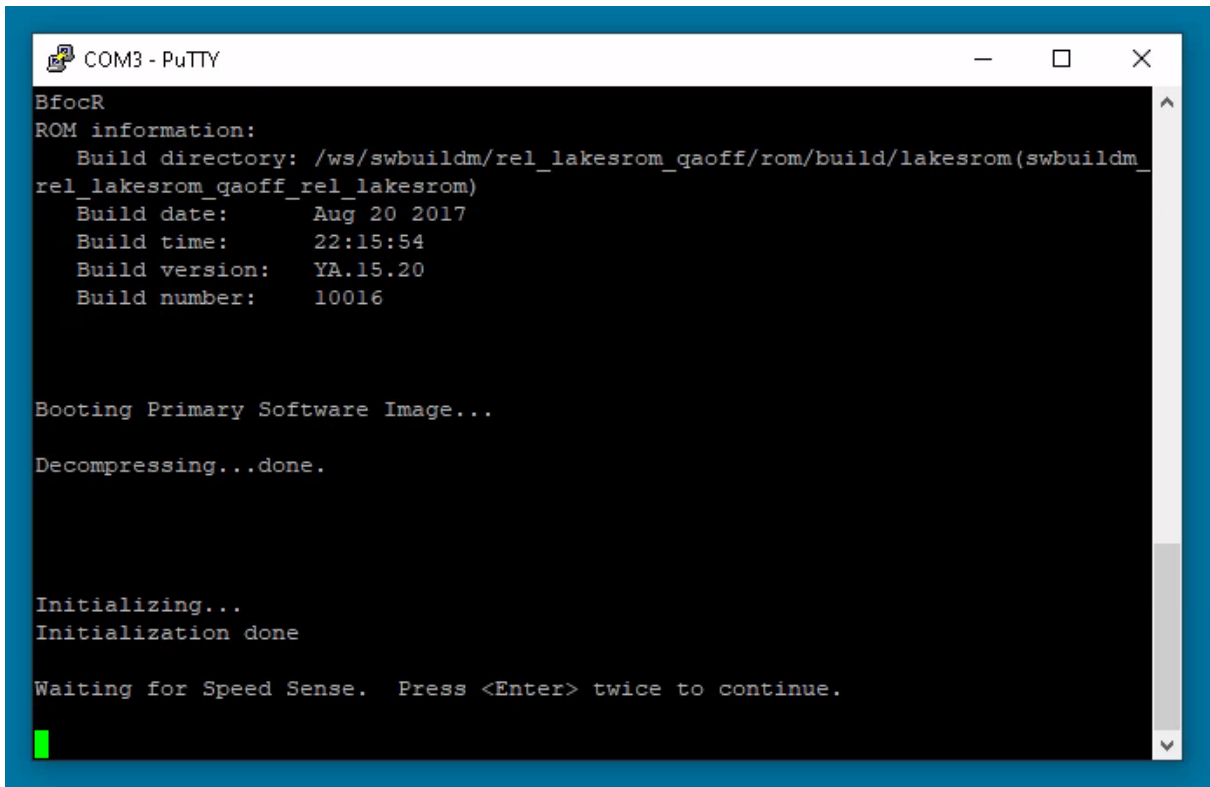


Abbildung 5: Zurücksetzen des Switches

Das Zurücksetzen hat ca. 3 Minuten gedauert.



```
COM3 - PuTTY
BfocR
ROM information:
  Build directory: /ws/swbuildm/rel_lakesrom_gaoff/rom/build/lakesrom(swbuildm_
rel_lakesrom_gaoff_rel_lakesrom)
  Build date:      Aug 20 2017
  Build time:      22:15:54
  Build version:   YA.15.20
  Build number:    10016

Booting Primary Software Image...

Decompressing...done.

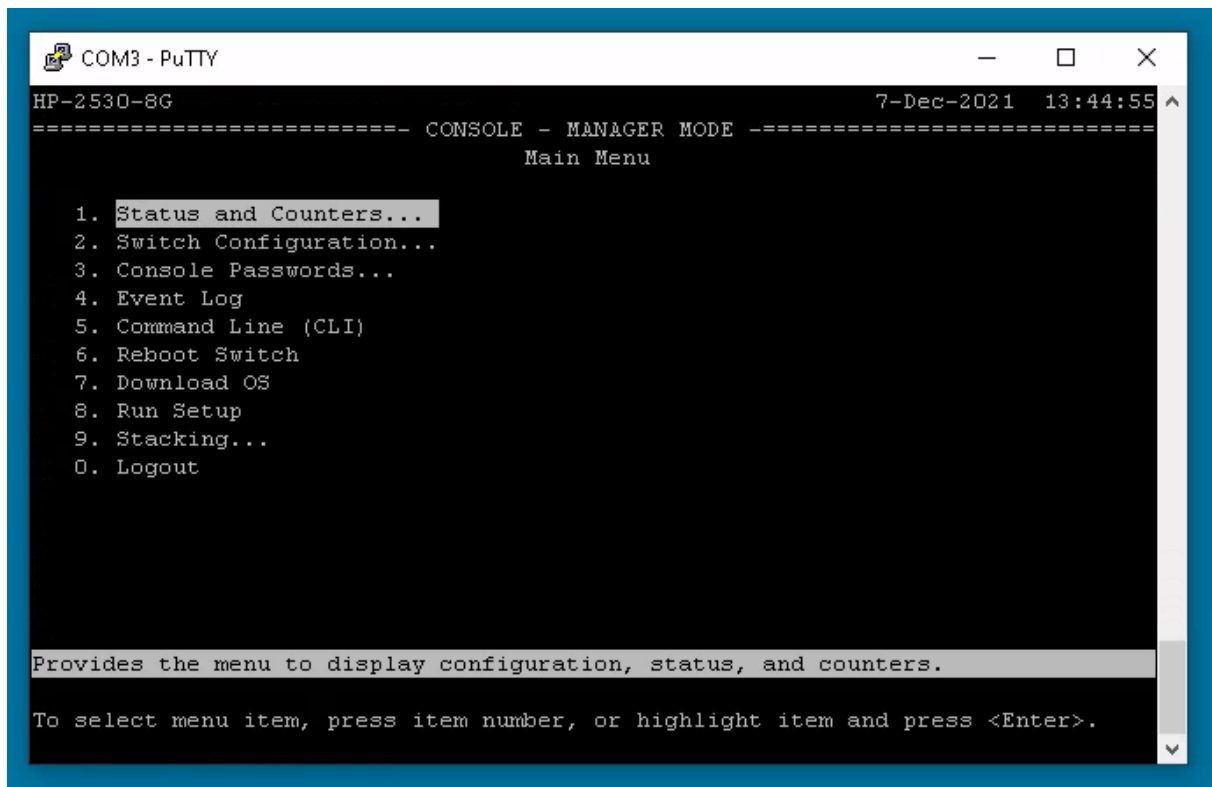
Initializing...
Initialization done

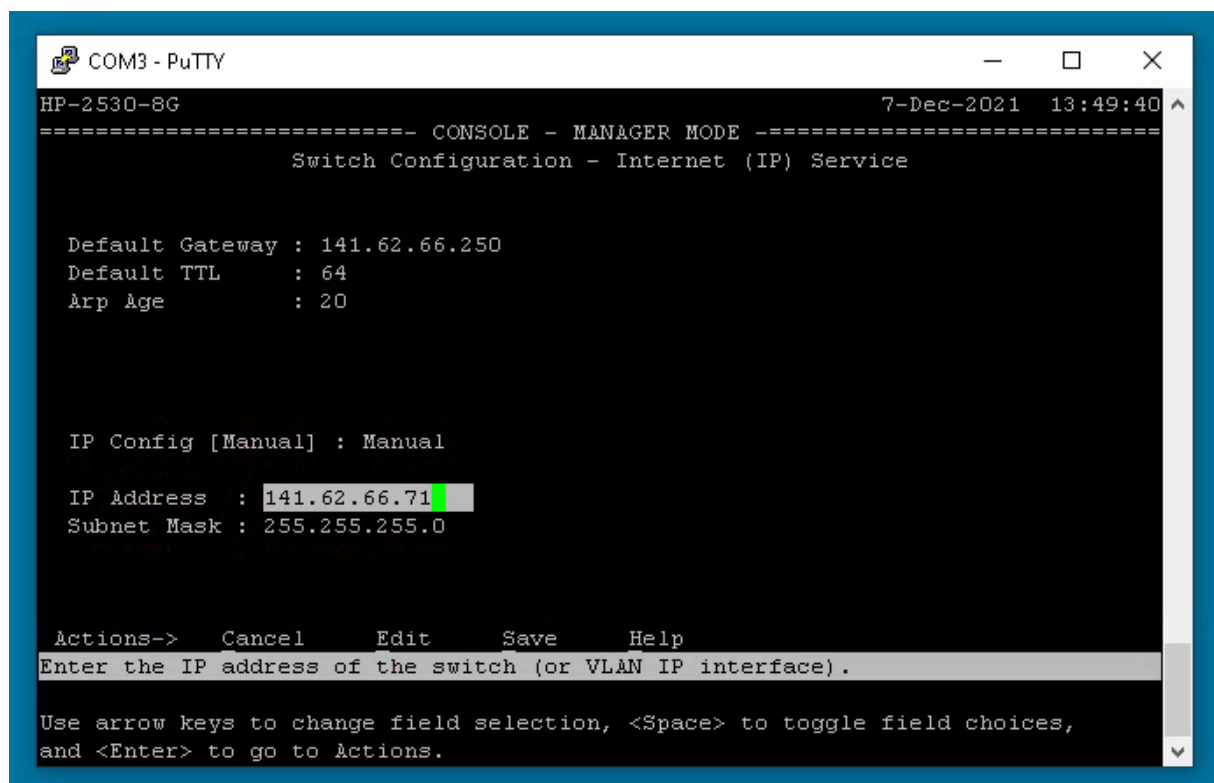
Waiting for Speed Sense.  Press <Enter> twice to continue.
```

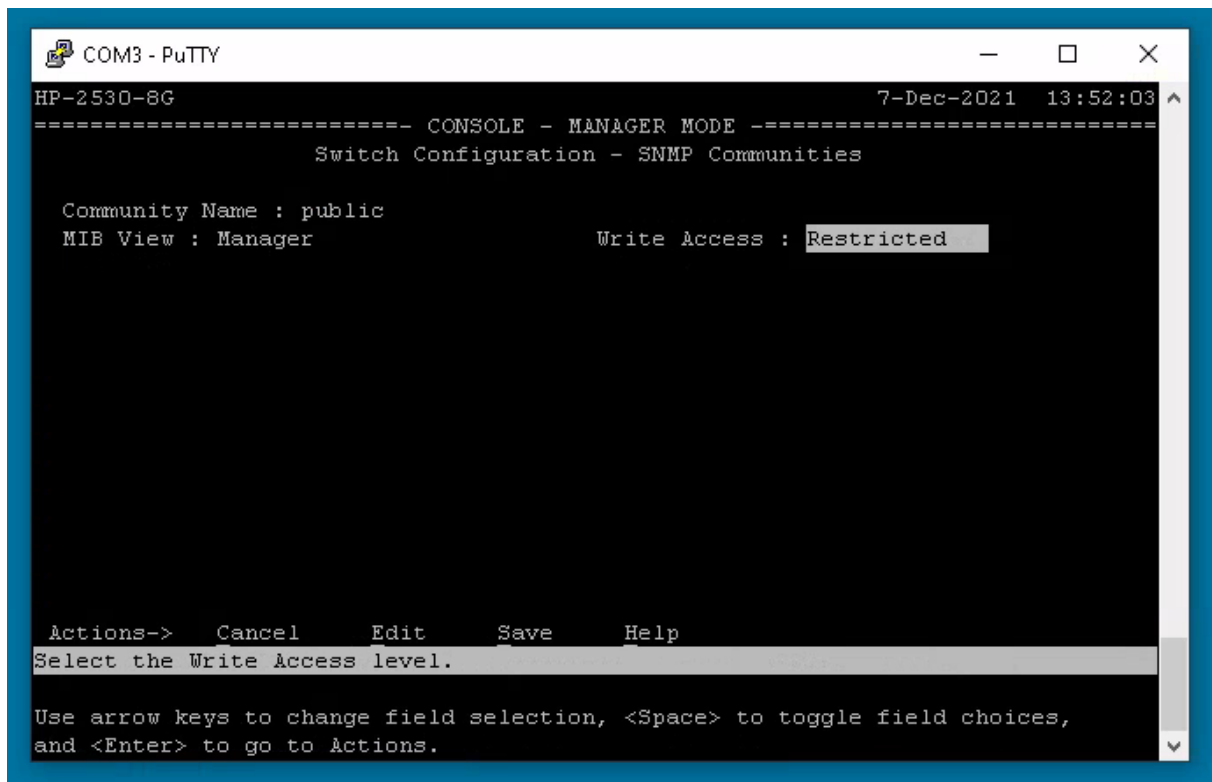
Abbildung 6: Nach dem Zurücksetzen des Switches

Vergeben Sie für Ihren Switch die entsprechende IP (siehe Zuordnung unter Ilias).

Der Switch wurde nach folgender Zuordnung angeschlossen: **switch-71** (141.62.66.71) ist per seriellm Kabel an rn01 angeschlossen

**Abbildung 7:** Main-Menü

**Abbildung 8:** IP-Konfiguration

**Abbildung 9:** SNMP-Konfiguration

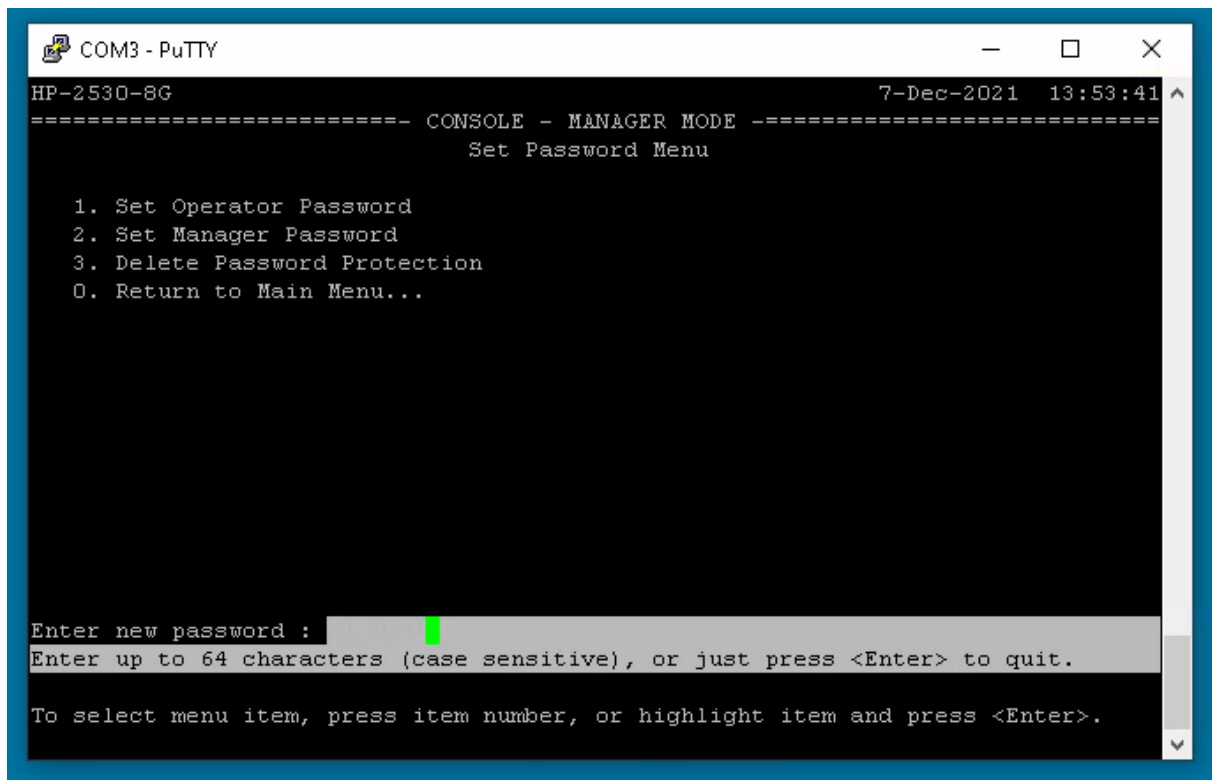


Abbildung 10: Einstellen des Passworts auf `versuch`

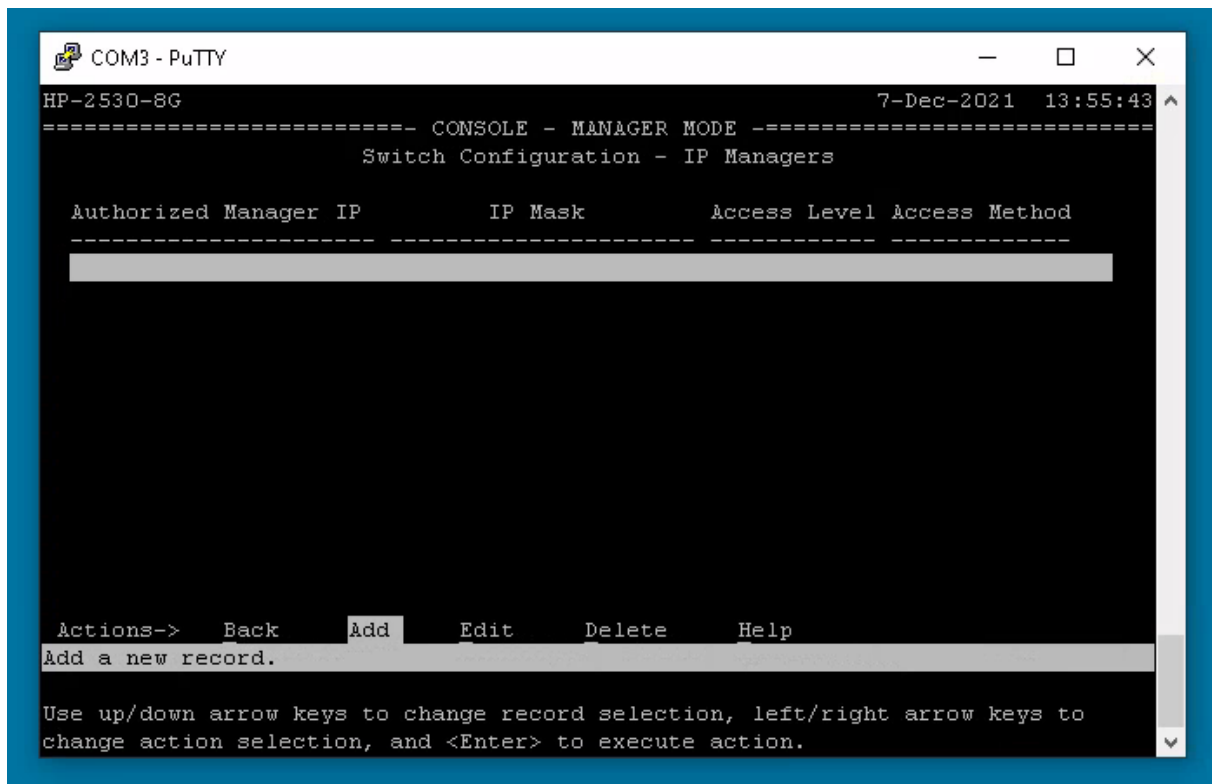
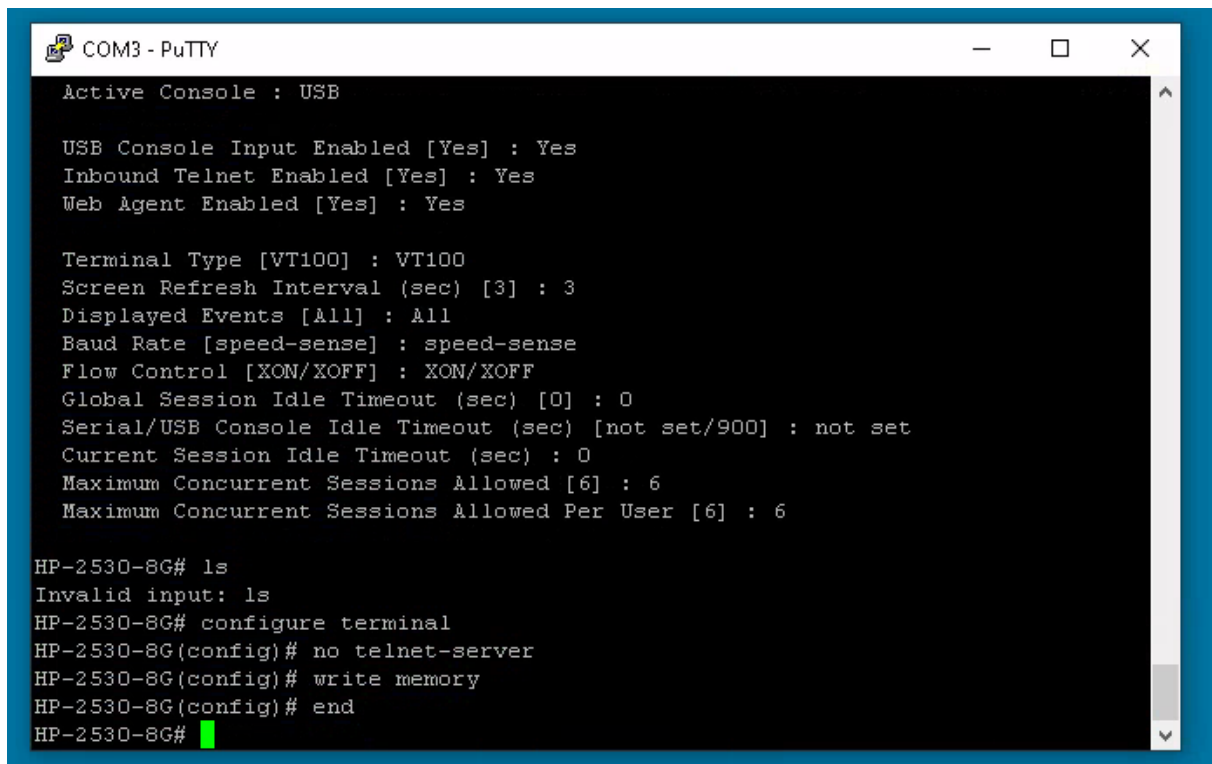


Abbildung 11: Telnet ist deaktiviert



```
COM3 - PuTTY
Active Console : USB

USB Console Input Enabled [Yes] : Yes
Inbound Telnet Enabled [Yes] : Yes
Web Agent Enabled [Yes] : Yes

Terminal Type [VT100] : VT100
Screen Refresh Interval (sec) [3] : 3
Displayed Events [All] : All
Baud Rate [speed-sense] : speed-sense
Flow Control [XON/XOFF] : XON/XOFF
Global Session Idle Timeout (sec) [0] : 0
Serial/USB Console Idle Timeout (sec) [not set/900] : not set
Current Session Idle Timeout (sec) : 0
Maximum Concurrent Sessions Allowed [6] : 6
Maximum Concurrent Sessions Allowed Per User [6] : 6

HP-2530-8G# ls
Invalid input: ls
HP-2530-8G# configure terminal
HP-2530-8G(config)# no telnet-server
HP-2530-8G(config)# write memory
HP-2530-8G(config)# end
HP-2530-8G#
```

Abbildung 12: Telnet ist durch Config deaktiviert

Nach der IP-Konfiguration ist ihr Switch auch über einen Web-Browser erreichbar. Neuerdings bietet HP dazu zwei unterschiedliche GUIs an. Schauen Sie sich diese beiden GUIs an und bilden Sie sich ein Urteil.

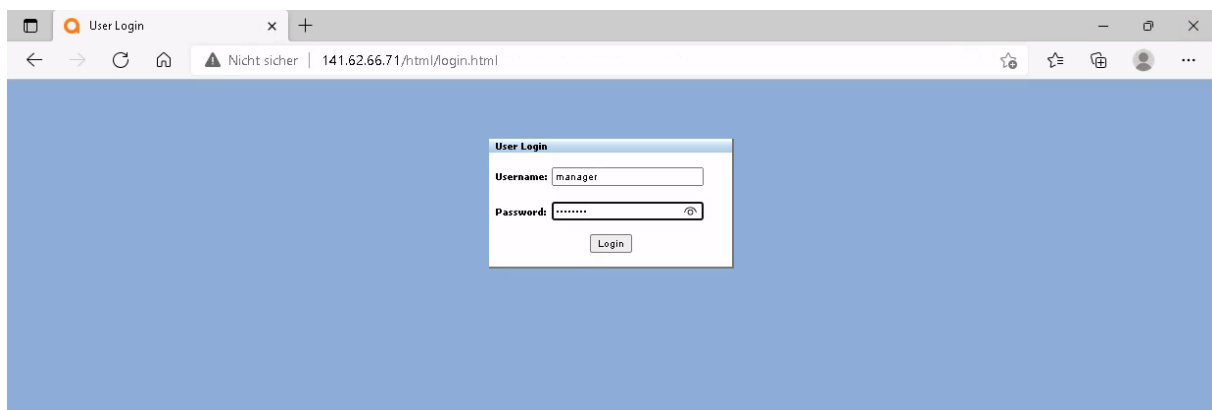


Abbildung 13: Login in die UI

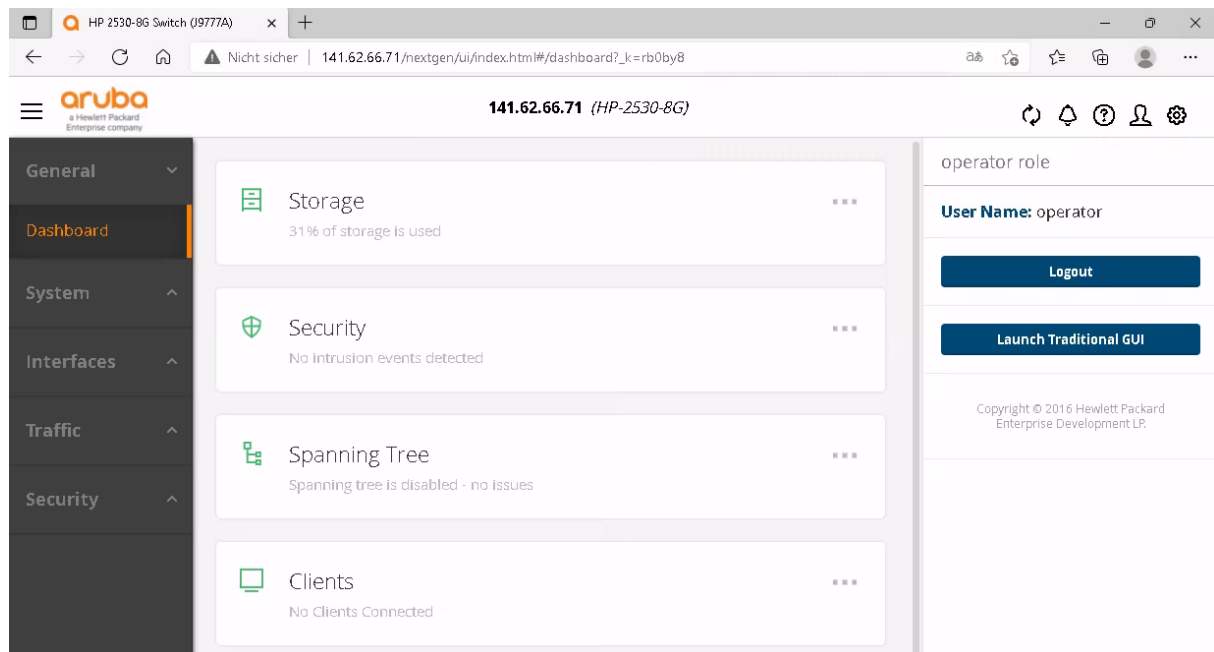


Abbildung 14: Neue UI

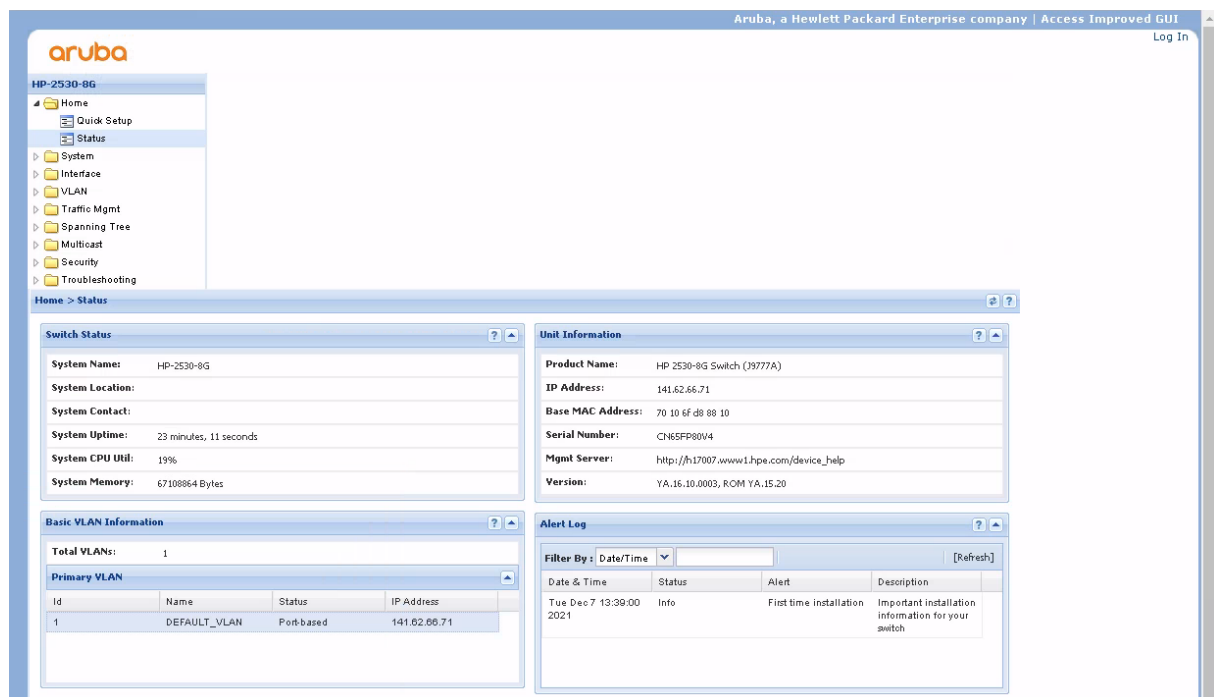


Abbildung 15: Alte UI

4 Analyse mit Wireshark

Starten Sie Wireshark und dokumentieren Sie die Protokolle die bereits jetzt Traffic in Zusammenhang mit ihrem Switch erzeugen (abgesehen von ihren eigenen httpAnfragen und die ARP-Anfragen von 141.62.66.236 (=FOG-Cloning Server) oder anderen Servern/Routern (=141.62.66.240, 141.62.66.250....) und natürlich dem RDP). Welchen Wireshark-Filter setzen Sie ein, um möglichst nur noch den Traffic ihres Switches einzufangen?

Mit dem Filter `!ip.addr && !arp` werden alle Pakete, welche keine IP-Adresse haben, und das ARP-Protokoll ausgeblendet; zurück bleibt nur noch der Traffic des Switches.

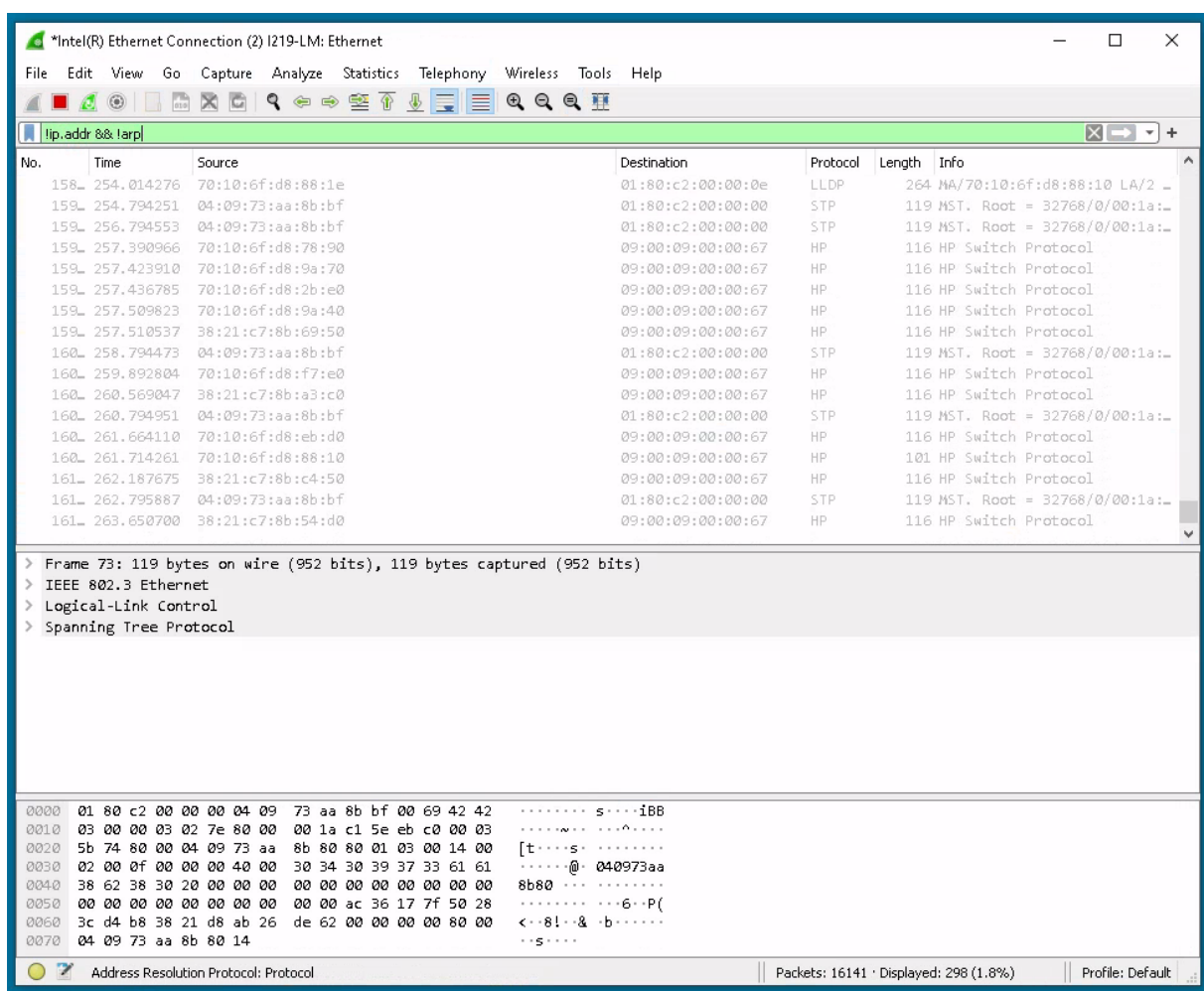


Abbildung 16: Traffic im Netzwerk des Switch

Was ist LLDP? Bringen Sie Ihren Windows-Client dazu, LLDP in Verbindung mit Ihrem Switch zu realisieren (Dafür ist unter Windows noch der LLDP-Dienst z.B. von <https://raspi.github.io/projects/winlldpserv>

zu installieren. Unter Linux lässt sich mit apt install lldpd der Dienst ebenfalls nachinstallieren.)

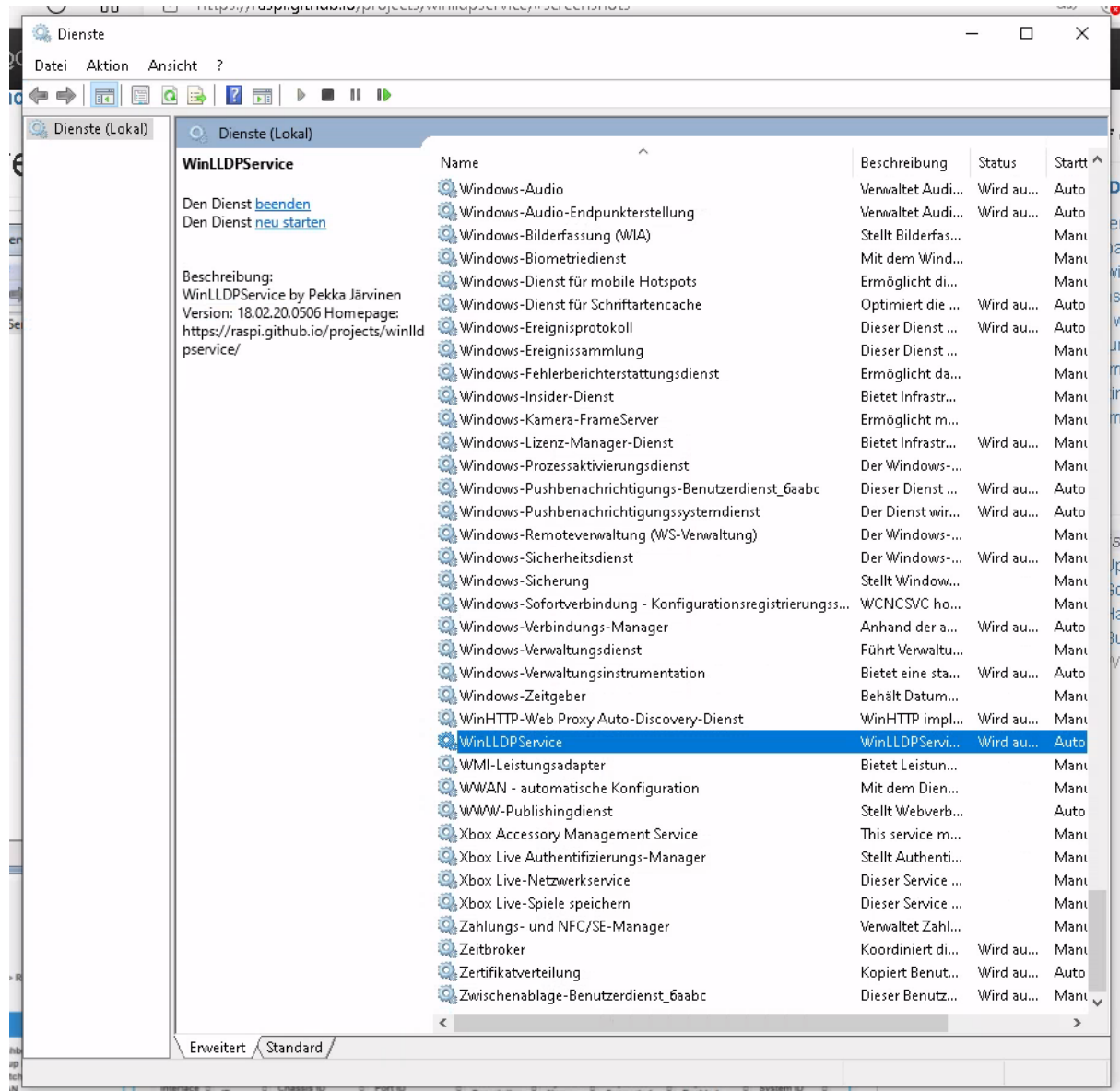


Abbildung 17: Start des LLDP-Dienstes

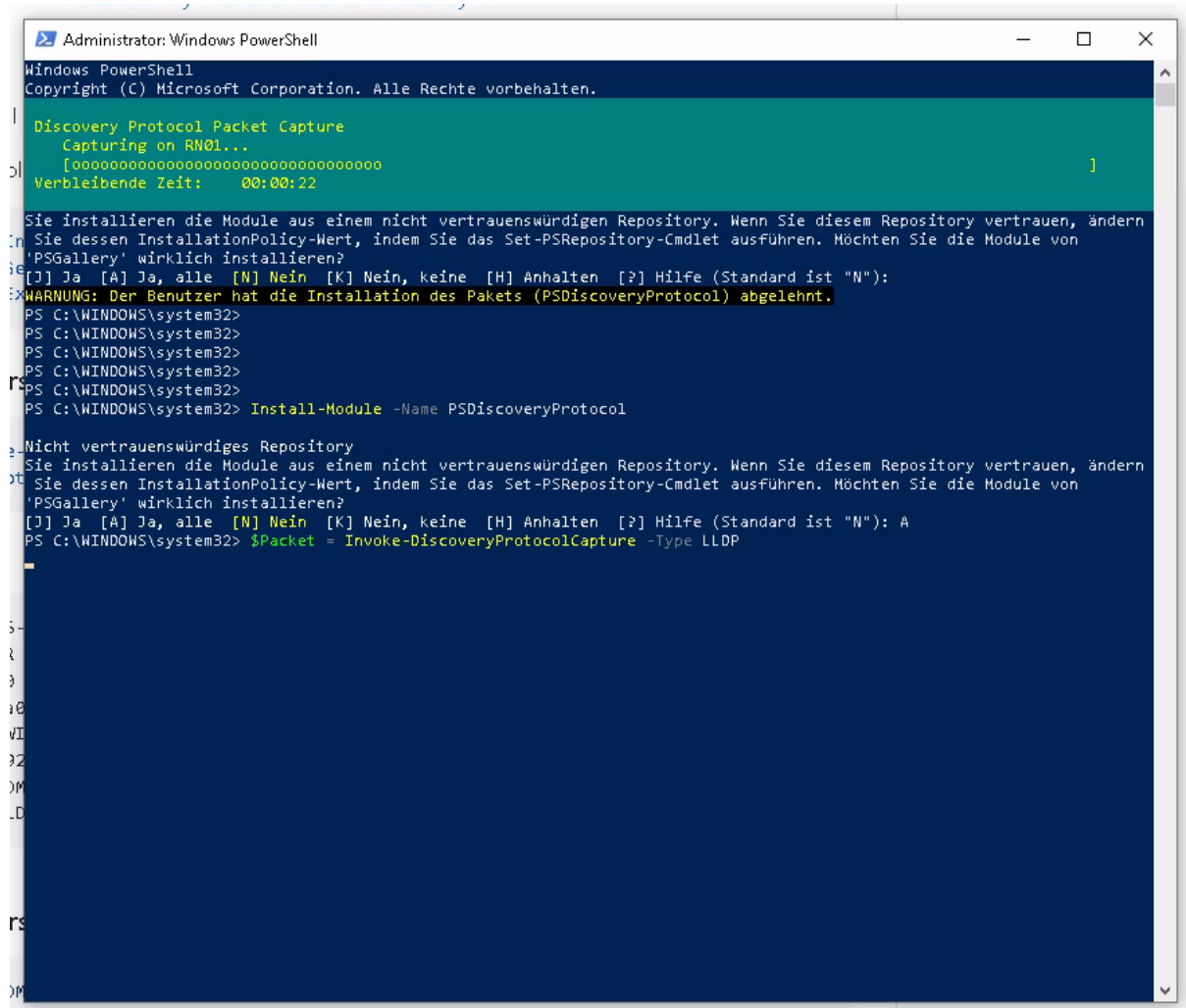


Abbildung 18: Auslesen eines LLDP-Pakets mittels PowerShell

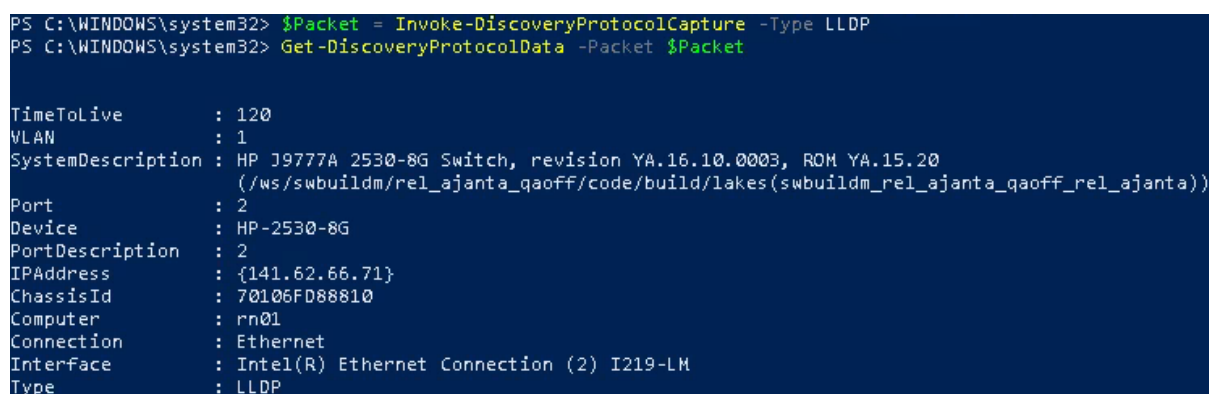


Abbildung 19: Darstellung eines LLDP-Pakets mittels PowerShell

5 Konfigurationsdatei

Laden Sie sich die Switch-Konfiguration auf ihren PC und schauen Sie sich die Datei mit einem Texteditor an.

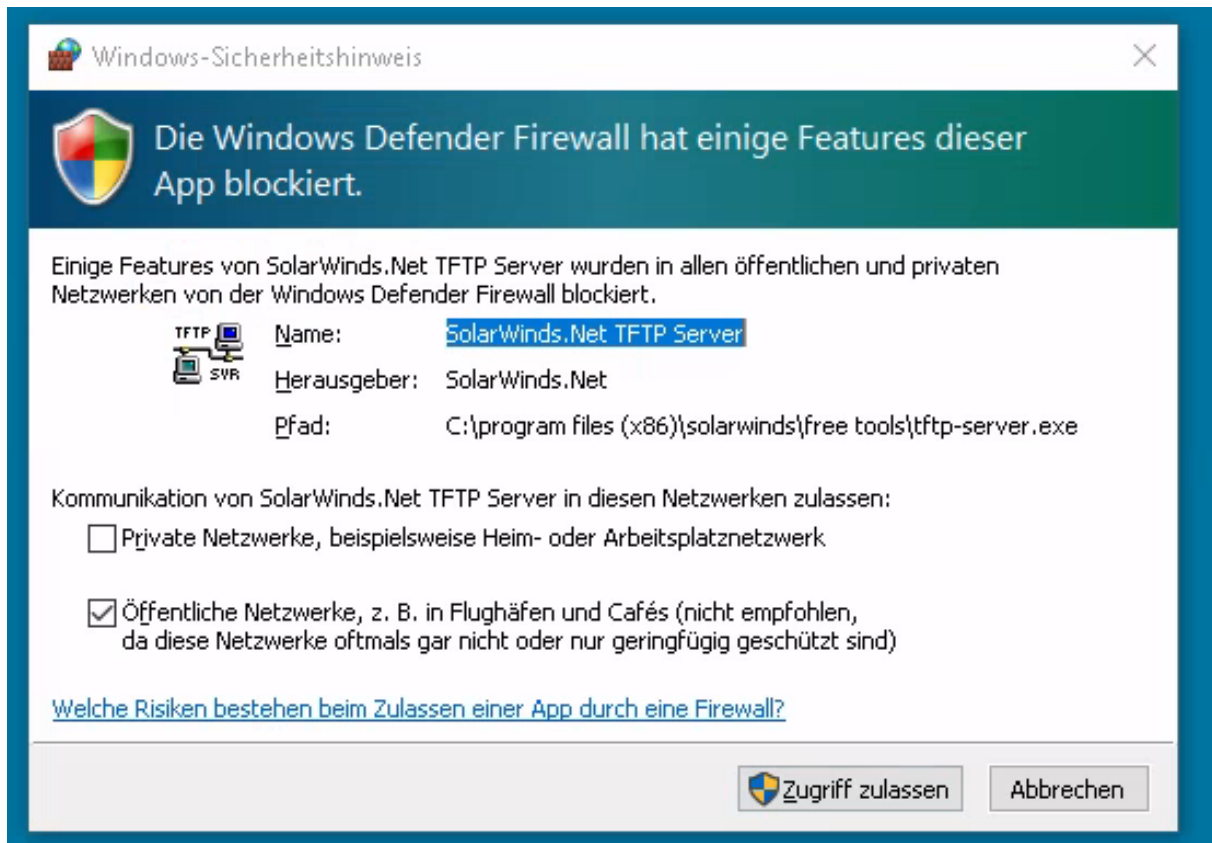


Abbildung 20: Start des TFTP-Servers auf der Workstation

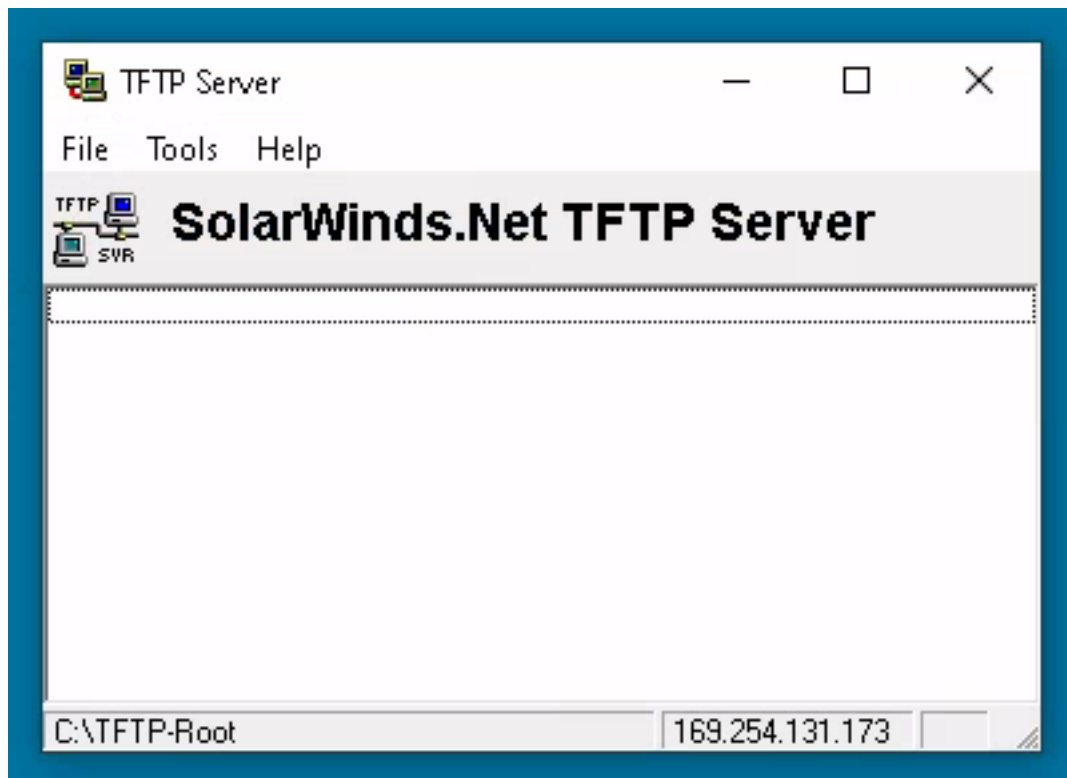


Abbildung 21: Gestarter TFTP-Server

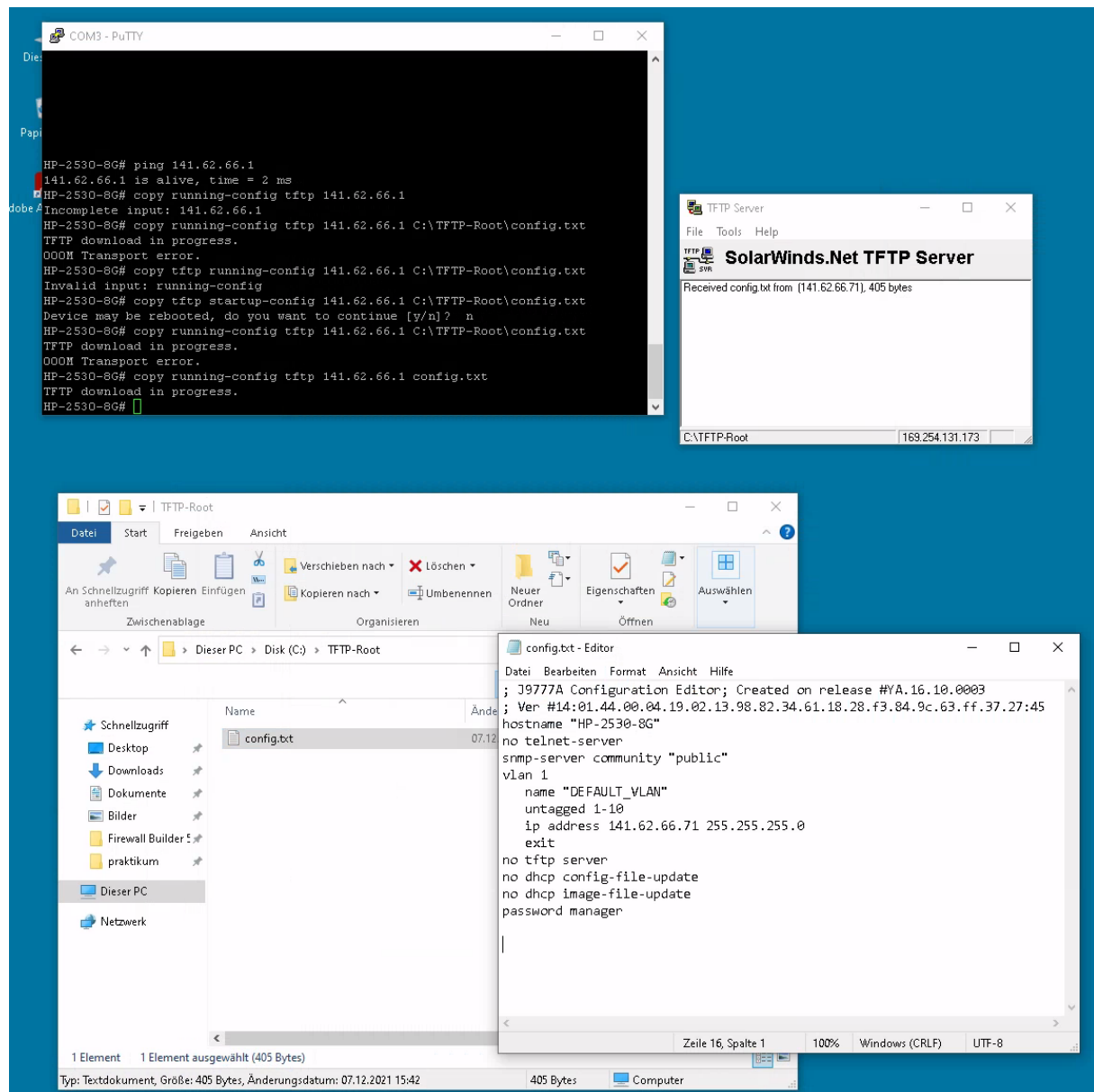


Abbildung 22: Upload der Config-Datei auf TFTP-Server

Ändern Sie in der heruntergeladenen Config-Datei den Namen des VLAN 1 und spielen Sie diese Datei als Konfiguration zurück auf den Switch.

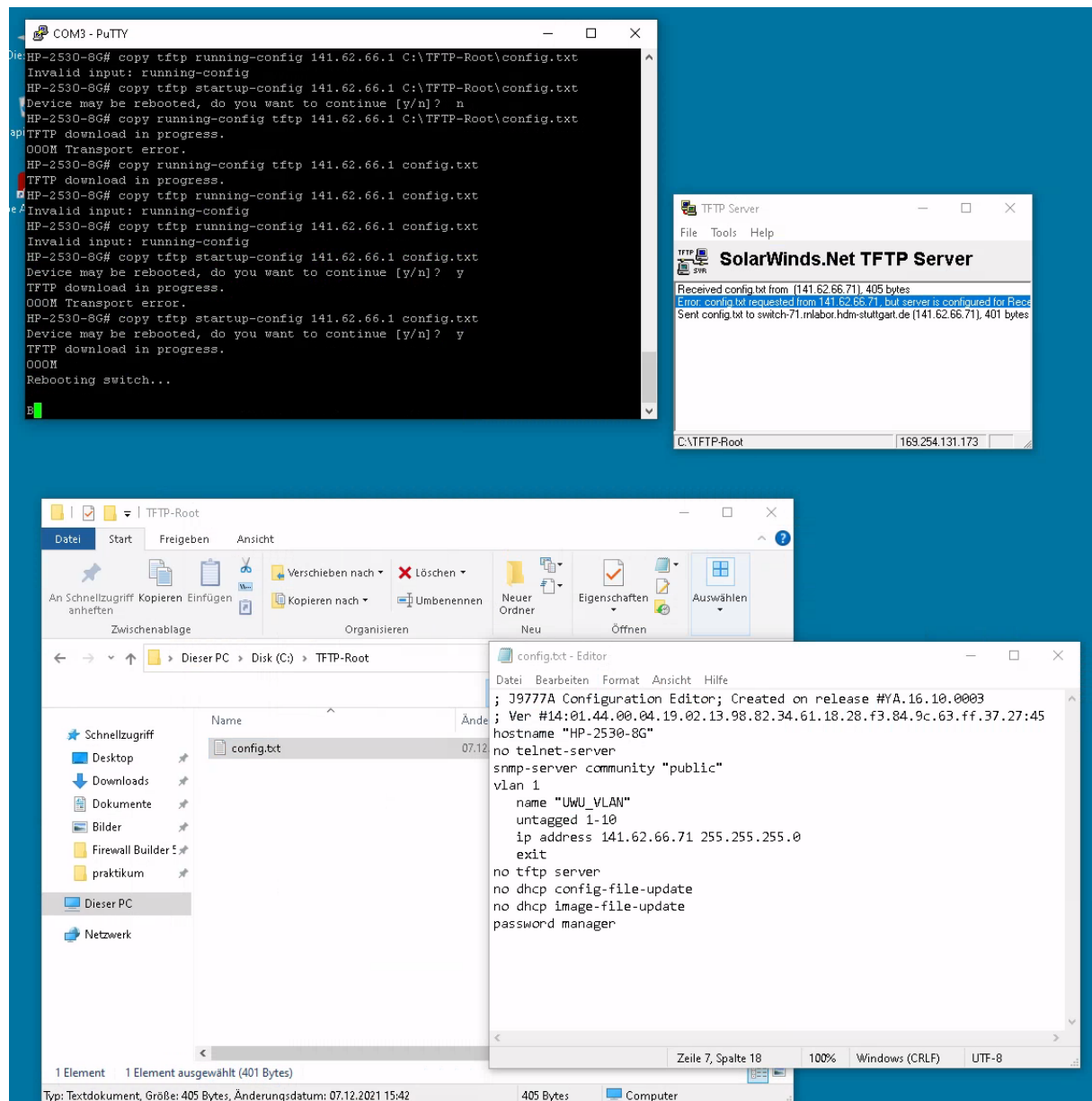
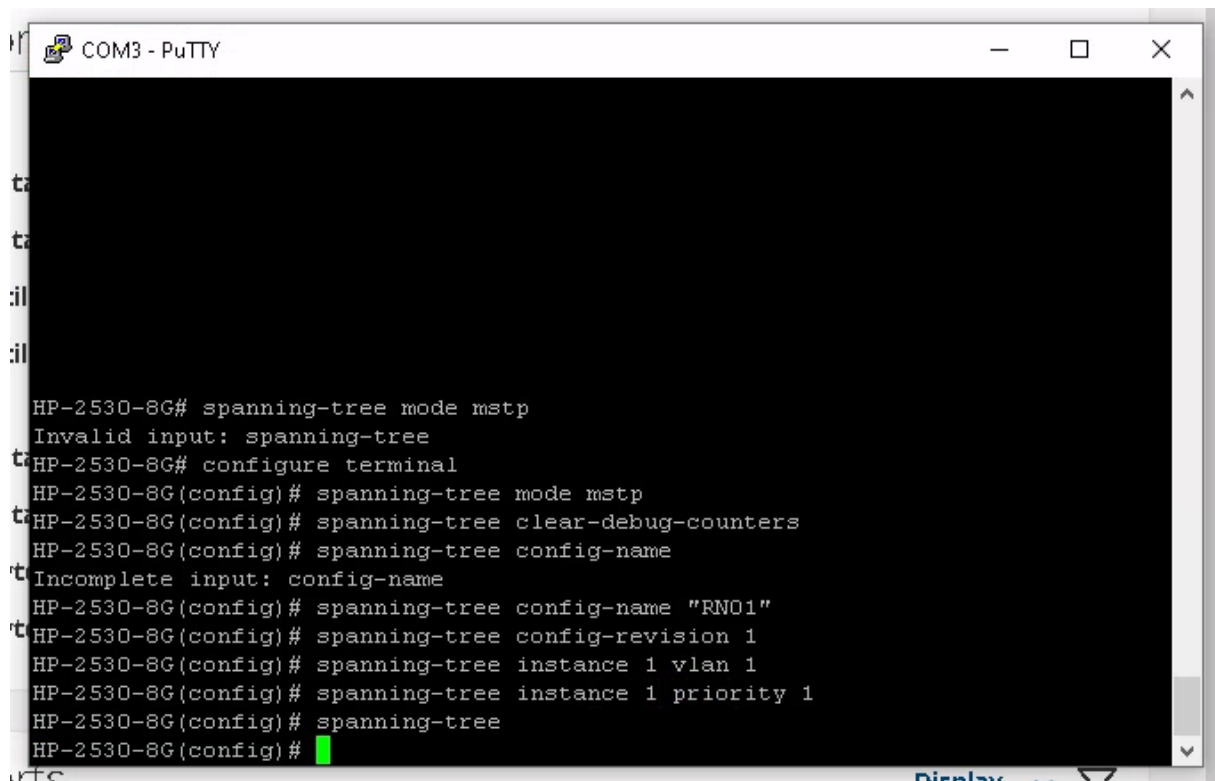


Abbildung 23: Download der geänderten Konfig-Datei vom TFTP-Server

6 Spanning-Tree-Verfahren

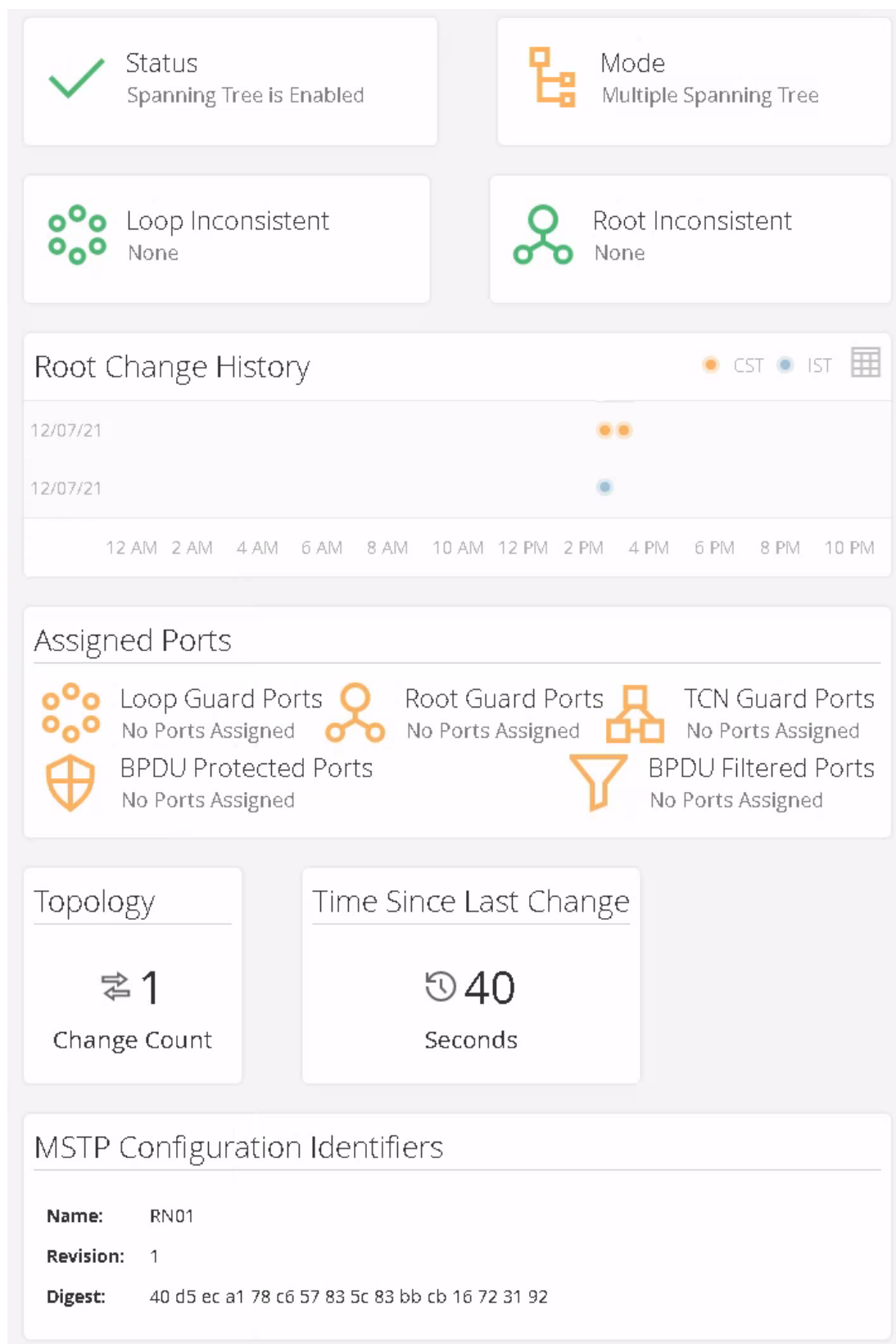
Aktivieren Sie das Spanning-Tree-Protokoll (Versuchen Sie herauszufinden was in ihrem Fall einzustellen ist, MSTP oder RSTP, wo liegen die Unterschiede). Stecken Sie nun eine Schleife (Der Betreuer im Labor erledigt das für sie) zwischen den Switches und versuchen Sie durch Verändern der Parameter, den Ring an einer Stelle zu unterbrechen (Hinweis: spanning-tree

priority)



```
COM3 - PuTTY
HP-2530-8G# spanning-tree mode mstp
Invalid input: spanning-tree
HP-2530-8G# configure terminal
HP-2530-8G(config)# spanning-tree mode mstp
HP-2530-8G(config)# spanning-tree clear-debug-counters
HP-2530-8G(config)# spanning-tree config-name
Incomplete input: config-name
HP-2530-8G(config)# spanning-tree config-name "RNO1"
HP-2530-8G(config)# spanning-tree config-revision 1
HP-2530-8G(config)# spanning-tree instance 1 vlan 1
HP-2530-8G(config)# spanning-tree instance 1 priority 1
HP-2530-8G(config)# spanning-tree
HP-2530-8G(config)#
```

Abbildung 24: Konfiguration des Spanning-Tree

**Abbildung 25:** UI-Ausgabe der Spanning-Tree-Konfiguration

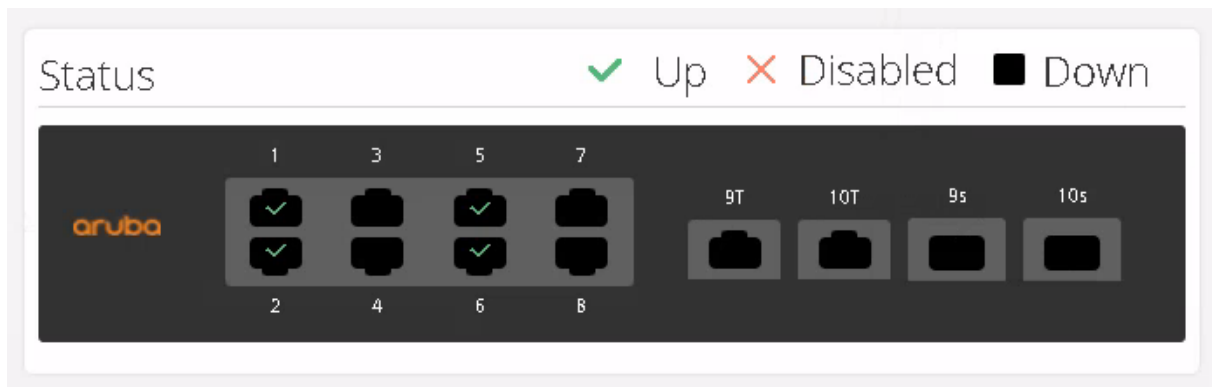


Abbildung 26: UI-Ausgabe der Ports nach dem Erstellen der Schleife

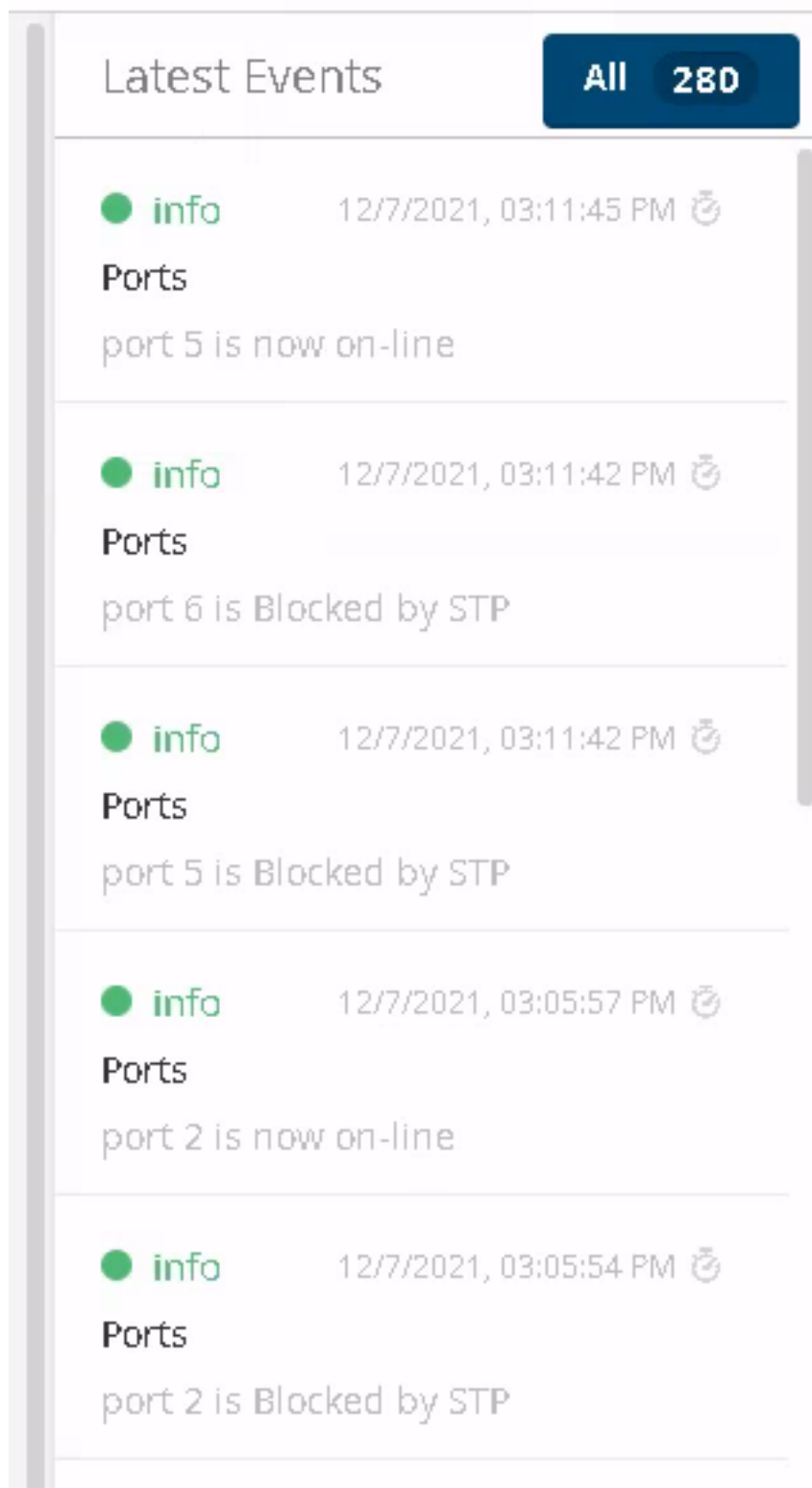


Abbildung 27: Ports werden automatisch durch MSTP blockiert

Welche Funktion hat das Protokoll BPDU (vgl. Anhang, Internet) in Zusammenhang mit Switches? In welchen Abständen sendet es der Switch? Was will er damit erreichen?

TODO: Add interpretation

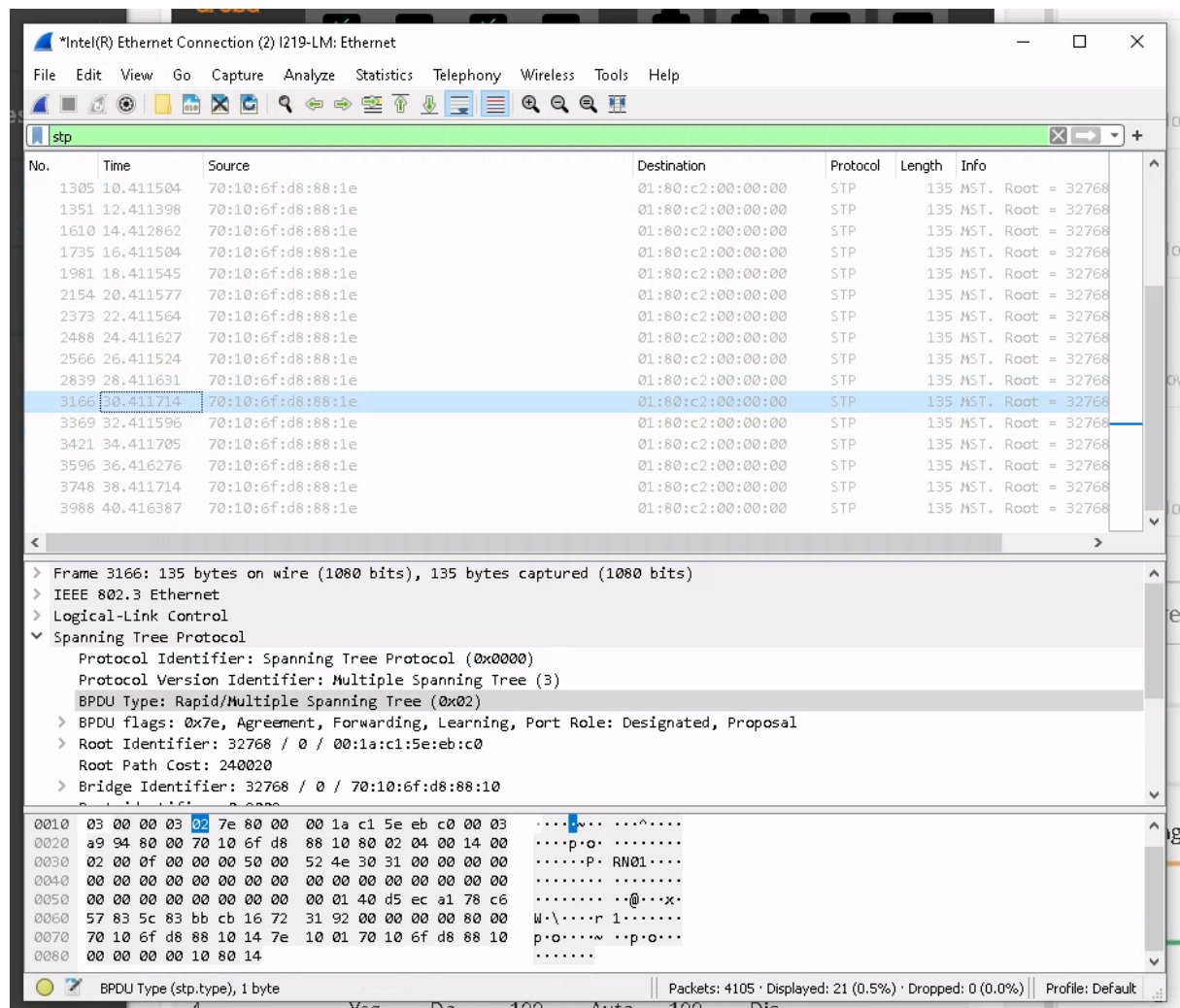


Abbildung 28: BPDU-Pakete werden alle 2 Sekunden gesendet

Dokumentieren und interpretieren Sie die Ziel-MAC-Adresse, an die die BPDU-Pakete gesendet werden.

TODO: Add interpretation

Ziel-MAC-Adresse: 01:80:c2:00:00:00

Die Adresse wird beschrieben als "Local LAN Segment, stopping at STP-capable switches".

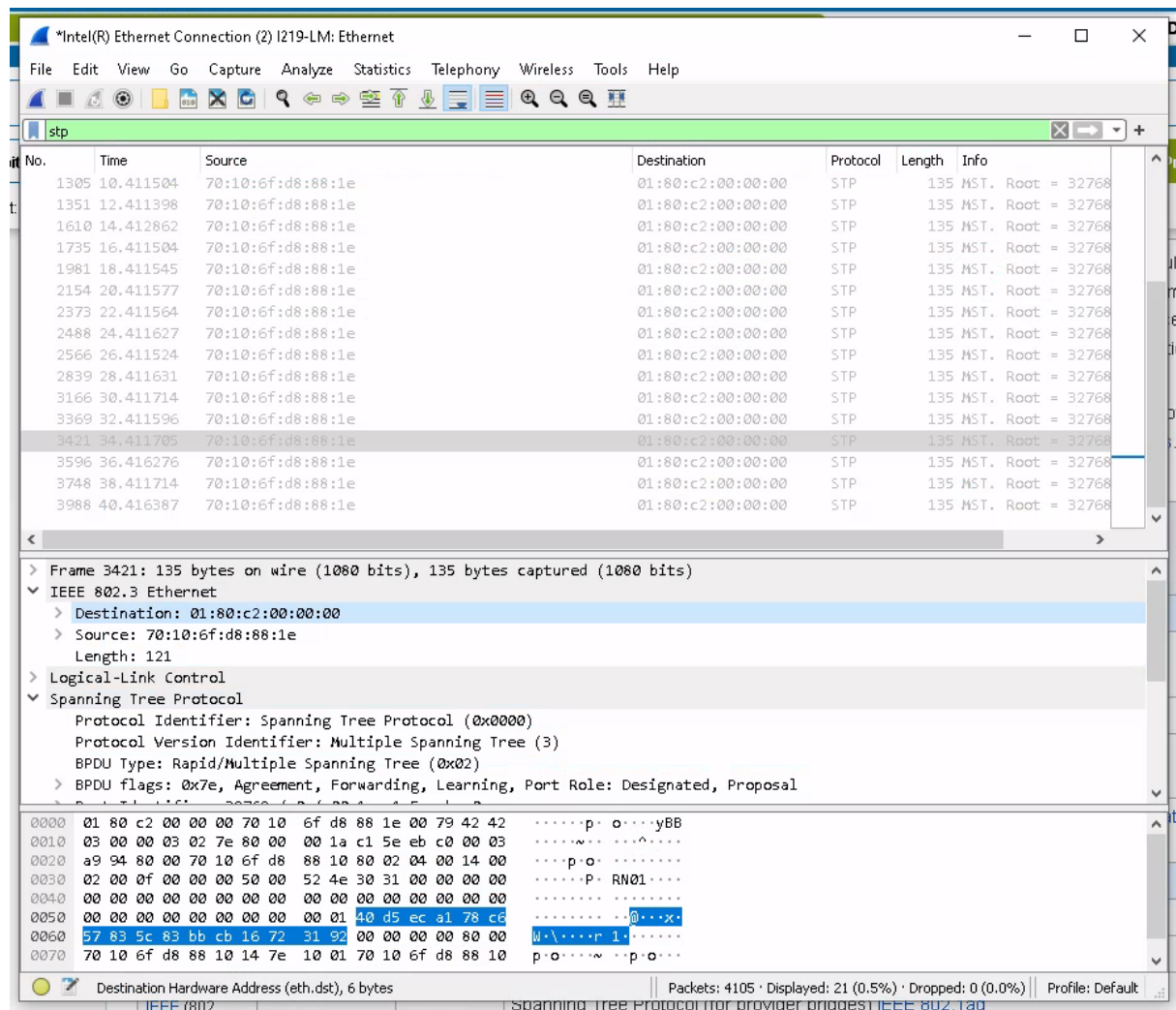


Abbildung 29: Ziel-MAC-Adresse eines BDPUs-Pakets

Mit Hilfe von `admin-edge-port` kann man für einzelne Switchports das Forwarding aktivieren. Diese Option bringt einen Port sofort in den Forwarding-Zustand, unabhängig davon ob evtl. Schleifen vorhanden sind oder nicht. Wo ist diese Funktion sinnvoll einsetzbar? Was ist der Unterschied zu der Option `auto-edge-port`? Welche Befehle gibt es sonst noch um sich den Status des Spanning-Tree anzusehen (Der Befehl `show` und seine Optionen helfen weiter)?

TODO: Add answer

7 Port Mirroring und Port Security

Spiegeln Sie den Datenverkehr eines beliebigen aktiven Ports auf einen anderen Port und dokumentieren Sie die Einstellung. Wann wird in der Praxis „Mirroring“ verwendet? Die entsprechende Funktion finden Sie unter Troubleshooting in der Web-Navigation links

TODO: Add answer



Abbildung 30: Deaktiviertes Port-Mirroring

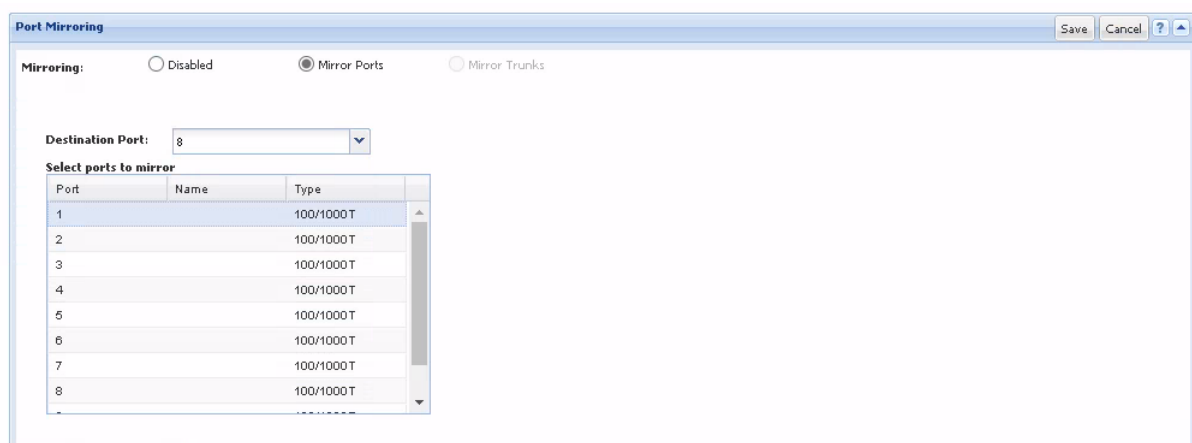


Abbildung 31: Einstellung Port-Mirroring von Port 1 auf Port 8

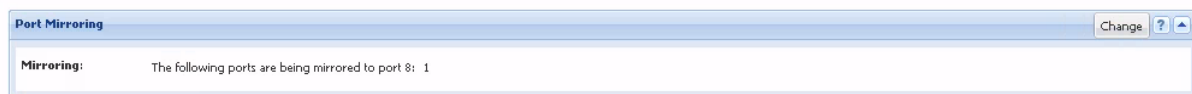


Abbildung 32: Aktiviertes Port-Mirroring

Überprüfen Sie, ob es möglich ist, alle Switch-Ports auf einen einzigen Port zu spiegeln. Wann ist dieses Vorgehen sinnvoll? Wo liegen die Grenzen?

TODO: Add answer

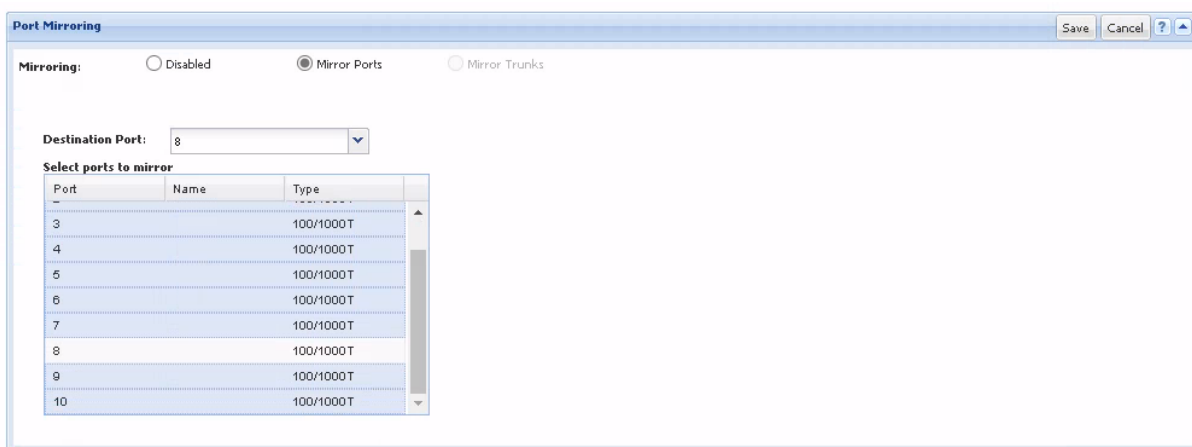


Abbildung 33: Einstellung Port-Mirroring alle Ports auf Port 8

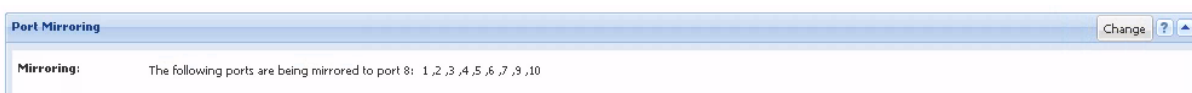


Abbildung 34: Aktiviertes Port-Mirroring alle Ports auf Port 8

Bei einem Switch können Sie aus Sicherheitsgründen den Zugriff auf erlaubte bzw. bekannte MAC-Adressen beschränken. Beispiel: Sie installieren einen Switch in Ihrer Firma und wollen, dass nur ausgewählte PCs (MAC-Adressen) in Ihrem Netzwerk kommunizieren können. Mitarbeiter dürfen keine privaten Geräte anschließen. Vorgehen: Sie konfigurieren die Port-Security für Port 8 und der Betreuer im Labor versucht über diesen Port mit einem Notebook (MAC-Adresse bitte erfragen) einen Ping ins Labor oder ins Internet.

Beispielhaft wird nur unsere Workstation (MAC-Adresse 4C:52:62:0E:E0:E6) allowlisted; theoretisch würde hier aber auch keine Adresse zum selben Effekt (keine Verbindung möglich).

Aktiviert wird "Send Trap and Disable", was zur Folge hat:

A trap is sent to all trap receivers when an unauthorized device is detected, and the unauthorized device is disabled.

Security Policy [Change] ?

Port(s): 8

Learn Mode: Static

Address Limit: 1

Violation Action: Send Trap and Disable

Authorized Addresses	
MAC ADDRESS	
4c5262-0ee0e6	

Abbildung 35: Aktivierte Port-Security auf Port 8 mit allowlisteter Workstation

Wie zu erwarten ist, konnte vor einem allowlisten ein angeschlossenes Laptop (MAC-Adresse 28:d2:44:e0:d9:28) nicht das Internet erreichen; wird dieser allerdings allowlisted, so kann dieses bzw. andere Hosts im Labor erreicht werden:

Port Security ?

Port	Port Name	Learn Mode	Address Limit	Violation Action
1		Continuous	1	None
2		Continuous	1	None
3		Continuous	1	None
4		Continuous	1	None
5		Continuous	1	None
6		Continuous	1	None
7		Continuous	1	None
8		Static	1	Send Trap and Disable
9		Continuous	1	None
10		Continuous	1	None

Security Policy [Change] ?

Port(s): 8

Learn Mode: Static

Address Limit: 1

Violation Action: Send Trap and Disable

Authorized Addresses	
MAC ADDRESS	
28d244-e0d928	

Abbildung 36: Aktivierte Port-Security auf Port 8 mit allowlistetem Laptop

8 VLANs

Erstellen sie auf dem Switch zwei weitere VLANs mit unterschiedlicher Priorität. Es befindet sich immer ein sogenanntes Default-VLAN auf einem Switch, welches meistens die ID 1 besitzt. Legen Sie ein VLAN 2 und ein VLAN 3 an und konfigurieren Sie auf Switch-Port 5 und 6 des Switches jeweils die drei VLANs als getagged. Was bedeutet in diesem Zusammenhang tagged und untagged?

TODO: Add answer

ID	Name	Status	Voice	Jumbo	IP Config	IP Address
1	UWU_VLAN	Port Based	No	No	Manual	141.62.66.71
2	WWW_VLAN	Port Based	No	No	Disabled	
3	WWW_VLAN	Port Based	No	No	Disabled	

VLAN 1	
VLAN Properties	
ID:	1
VLAN Name:	UWU_VLAN
Status:	Port Based
Primary VLAN:	Yes
Management VLAN:	No

Ports	
Tagged (Static):	5-6
Tagged (GVRP):	None
Untagged:	1-4,7-10
Forbidden:	None

Abbildung 37: VLAN 1

Abbildung 38: VLAN 2

VLAN Table

Add VLANDelete VLAN

Filter By: ID

ID	Name	Status	Voice	Jumbo	IP Config	IP Address
1	UWU_VLAN	Port Based	No	No	Manual	141.62.66.71
2	VWV_VLAN	Port Based	No	No	Disabled	
3	WWW_VLAN	Port Based	No	No	Disabled	

Page 1 of 1

Displaying VLAN 1 - 3 of 3

VLAN 3

[Change]

VLAN Properties

ID: 3

VLAN Name: WWW_VLAN

Status: Port Based

Primary VLAN: No

Management VLAN: No

Ports

[Change]

Tagged (Static): 5-6

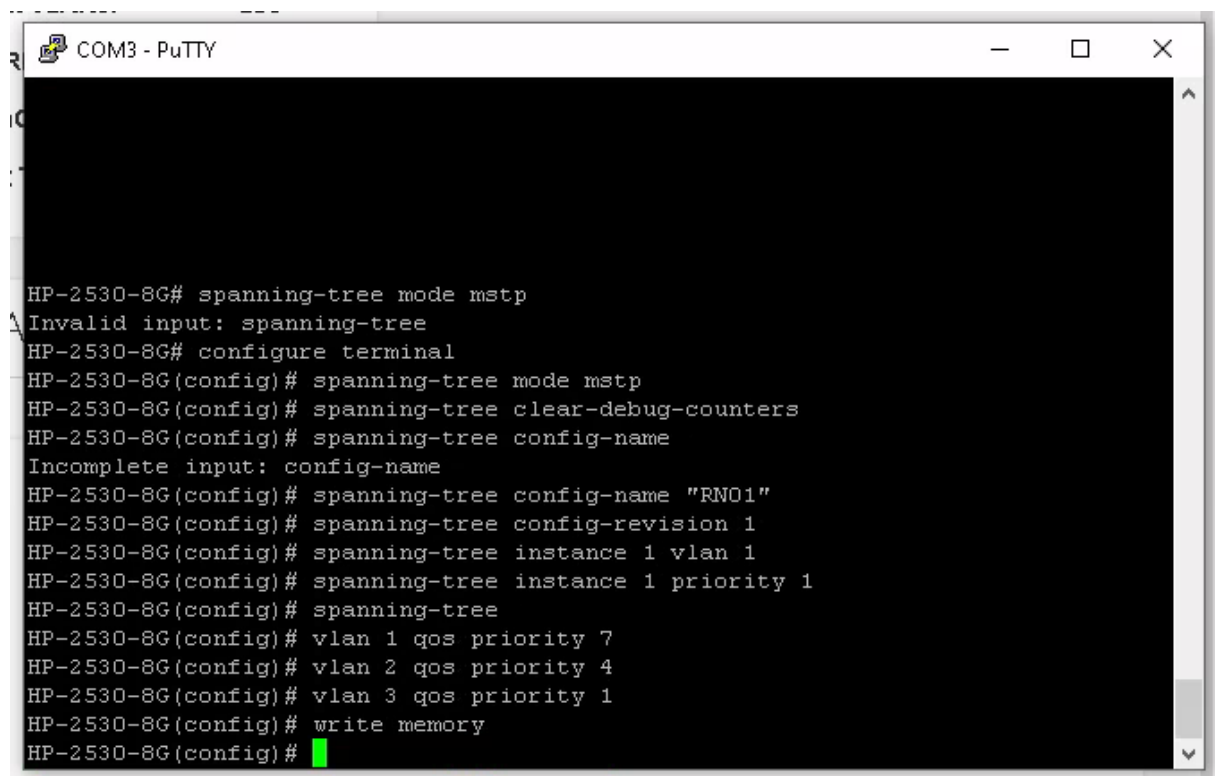
Tagged (GVRP): None

Untagged: None

Forbidden: None

Abbildung 39: VLAN 3

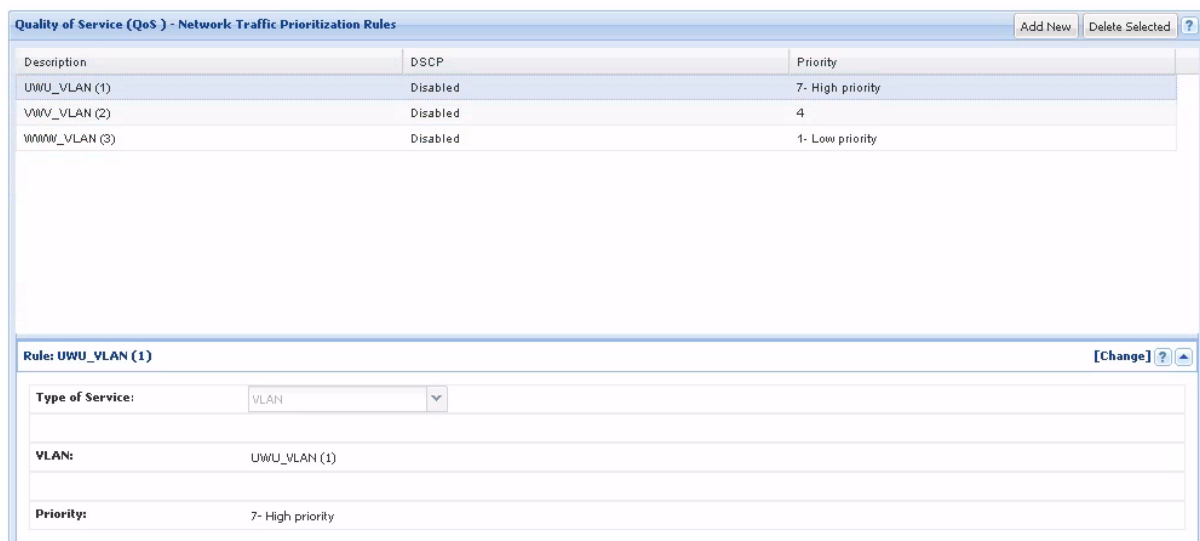
Es sollen über diese 2 Switch-Ports 3 VLANs bedient werden. Im weiteren setzen Sie für diese VLANs unterschiedlichen Prioritäten (Stichwort: qos)



```
HP-2530-8G# spanning-tree mode mstp
Invalid input: spanning-tree
HP-2530-8G# configure terminal
HP-2530-8G(config)# spanning-tree mode mstp
HP-2530-8G(config)# spanning-tree clear-debug-counters
HP-2530-8G(config)# spanning-tree config-name
Incomplete input: config-name
HP-2530-8G(config)# spanning-tree config-name "RNO1"
HP-2530-8G(config)# spanning-tree config-revision 1
HP-2530-8G(config)# spanning-tree instance 1 vlan 1
HP-2530-8G(config)# spanning-tree instance 1 priority 1
HP-2530-8G(config)# spanning-tree
HP-2530-8G(config)# vlan 1 qos priority 7
HP-2530-8G(config)# vlan 2 qos priority 4
HP-2530-8G(config)# vlan 3 qos priority 1
HP-2530-8G(config)# write memory
HP-2530-8G(config) #
```

Abbildung 40: VLAN-Config

Diese Konfiguration spiegelt sich auch im Web-Interface wieder:



Description	DSCP	Priority
UWU_VLAN (1)	Disabled	7- High priority
VWV_VLAN (2)	Disabled	4
WWW_VLAN (3)	Disabled	1- Low priority

Rule: UWU_VLAN (1) [Change] ?

Type of Service:

VLAN:

Priority:

Abbildung 41: VLAN-Config in der UI

Die VLAN-Priorisierung auf dem SmartClass Tester entspricht der VLAN-Konfiguration auf dem Switch. Was sollte ihrer Meinung mit den drei Streams passieren?

TODO: Add answer

Der Betreuer teilt Ihnen die Ergebnisse der Messung zur Dokumentation mit

Gemessen wurden wie erwartet folgende Werte, welche zusammen eine Datenrate von ~99.6 Mbit/s darstellen:

Stream	Datenrate
1	53 Mbit/s
2	41 Mbit/s
3	5.6 Mbit/s

Die UI zeigt hier auch den Traffic an:

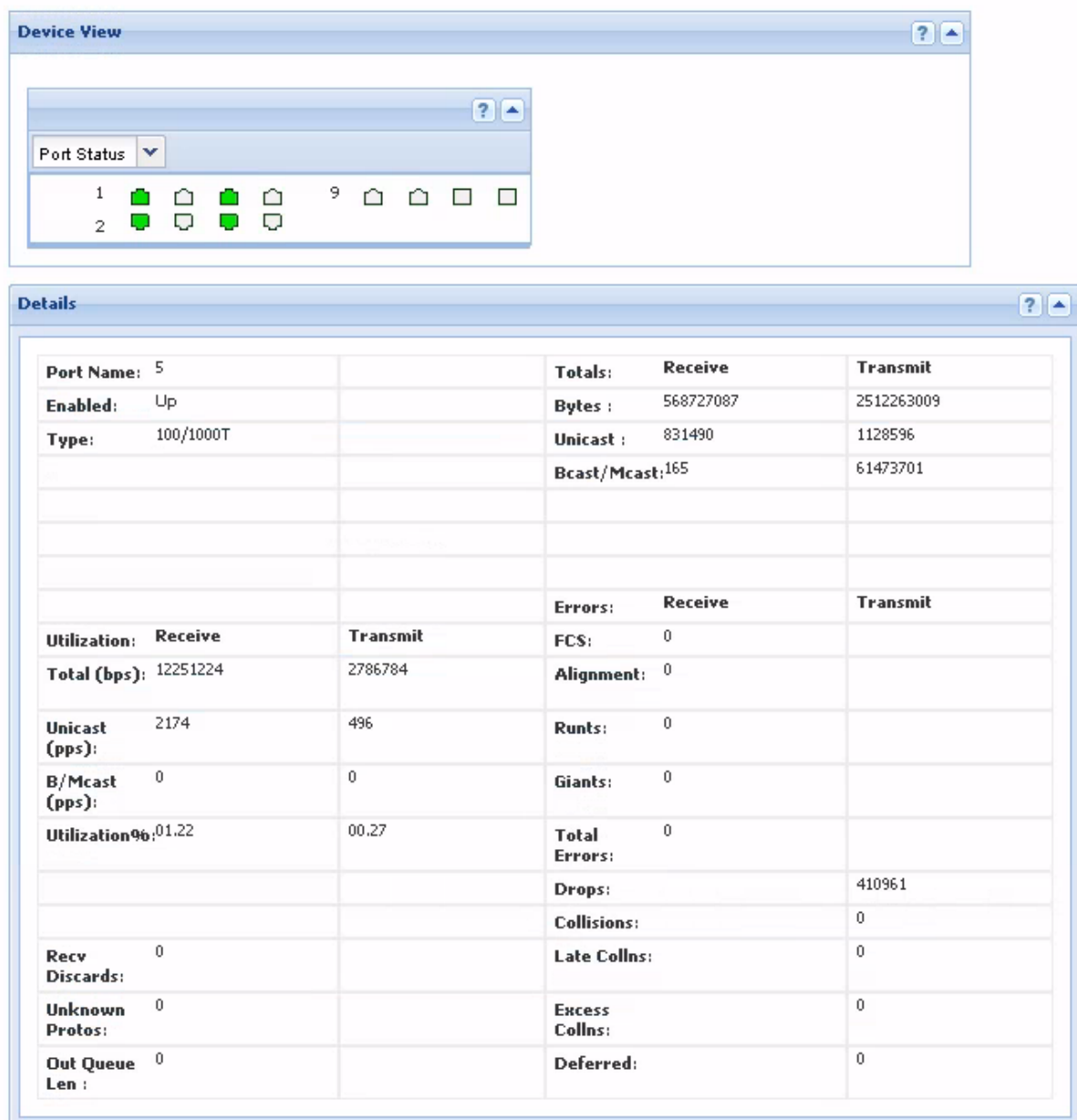
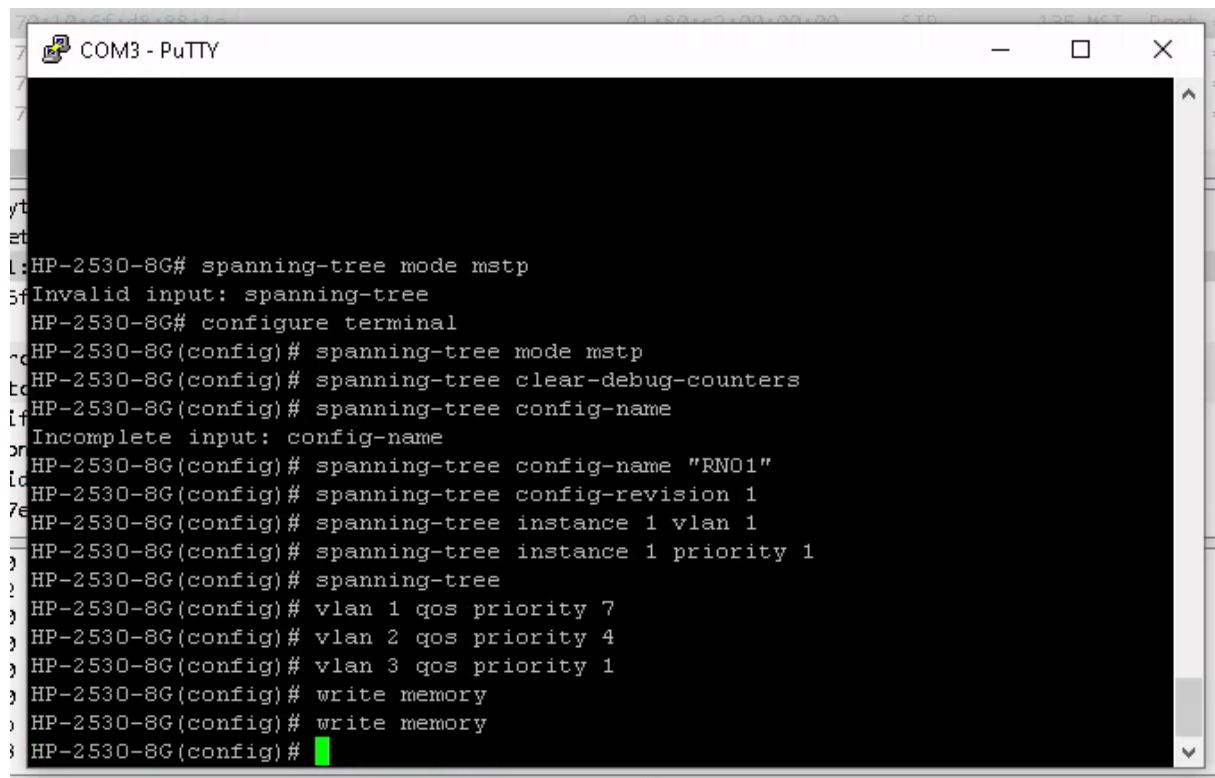


Abbildung 42: VLAN-Traffic in der UI

9 Sichern der Konfiguration

Sichern Sie Ihre Konfiguration mit: `write memory` bevor sie den Switch ausschalten und notieren Sie sich Ihre Switch-Nummer, im nächsten Versuch „Netzwerkmanagement“ werden Sie „Ihren“ Switch wieder brauchen.



```
COM3 - PuTTY
HP-2530-8G# spanning-tree mode mstp
Invalid input: spanning-tree
HP-2530-8G# configure terminal
HP-2530-8G(config)# spanning-tree mode mstp
HP-2530-8G(config)# spanning-tree clear-debug-counters
HP-2530-8G(config)# spanning-tree config-name
Incomplete input: config-name
HP-2530-8G(config)# spanning-tree config-name "RNO1"
HP-2530-8G(config)# spanning-tree config-revision 1
HP-2530-8G(config)# spanning-tree instance 1 vlan 1
HP-2530-8G(config)# spanning-tree instance 1 priority 1
HP-2530-8G(config)# spanning-tree
HP-2530-8G(config)# vlan 1 qos priority 7
HP-2530-8G(config)# vlan 2 qos priority 4
HP-2530-8G(config)# vlan 3 qos priority 1
HP-2530-8G(config)# write memory
HP-2530-8G(config)# write memory
HP-2530-8G(config)#
```

Abbildung 43: Speichern der Konfiguration