tcpdump zu lokalem Wireshark umleiten

tcpdump muss auf dem EdgeRouter installiert sein.tcpdump wird per SSH von remote gestartet und das Capture auf die Standardausgabe gelenkt. Gleichzeitig wird auf dem lokalen Host ein wireshark gestartet, das darüber seinen Input bezieht.

```
$ ssh admin@edgerouter 'sudo tcpdump -f -i switch0 -w -' | wireshark-gtk -k -i -
```

Je nach Desktop muss wireshark-gtk oder wireshark-qt verwendet werden.

Mittels plink aus dem Putty-Paket funktioniert das auch für Windows (pagent sollte laufen und der passende Key geladen sein):

```
plink -batch -l admin -P 22 edgerouter sudo /usr/bin/tshark -i switch0 -w -  | "c:\Program Files
```

Revision #1
Created 31 May 2021 14:50:13 by magenbrot
Updated 31 May 2021 14:50:31 by magenbrot