Netzwerk-Hardware für zu Hause

Professionelle Netzwerk-Hardware zum kleinen Preis hat auch für zu Hause viele Vorteile

Linux-Cafe 2020-11-11

Bernd Strößenreuther
mailto:linux-cafe@stroessenreuther.net

Lizenz

Agenda

1) Das Standard-Setup zu Hause

2) Professionelle Netzwerk-Hardware: Warum?

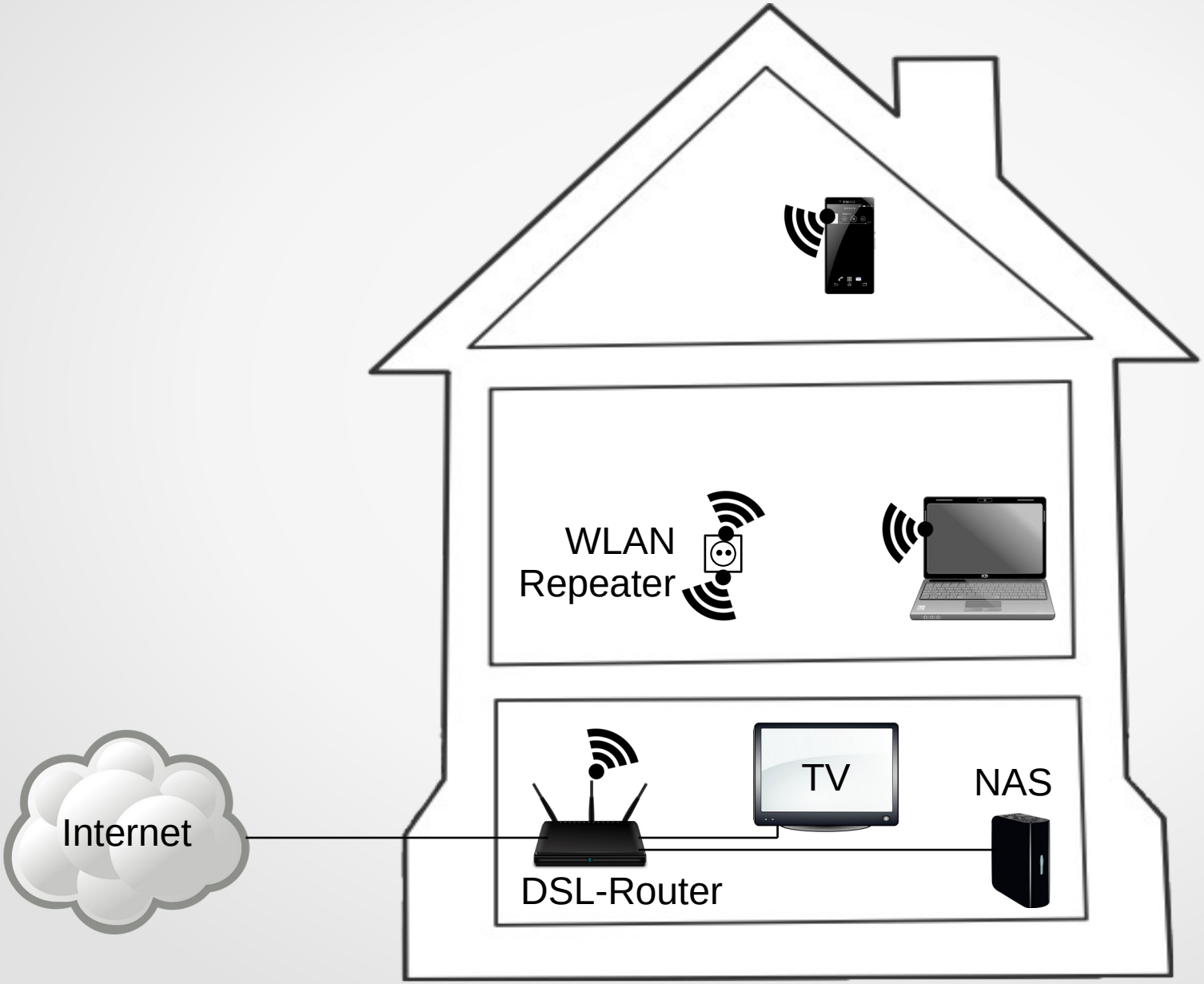
3) Möglichkeiten

Exkurs: VLANs

4) Live-Demo

Exkurs: QR-Code für WLAN-Zugriff

Das Standard-Setup zu Hause



Funktioniert gut

- WLAN im ganzen Haus
- 2,4 GHz + 5 GHz
- Separates Gäste-WLAN

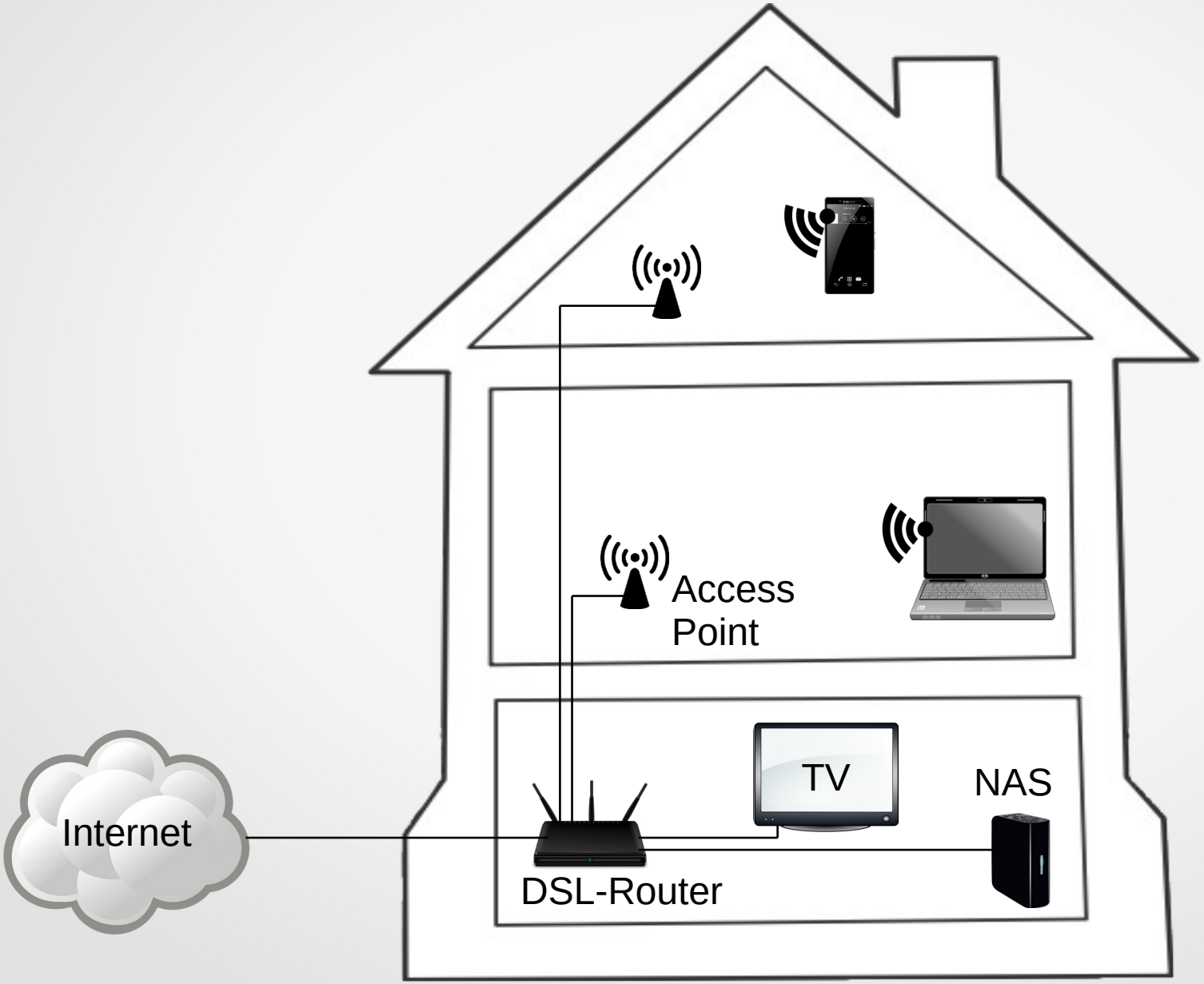
Warum soll ich etwas verändern?

- Mehr verfügbare Bandbreite im WLAN erforderlich
  - Home-Office + Home-Schooling: Mehrere Video-Konferenzen parallel sollen ohne Qualitätseinbußen möglich sein
- WLAN-“Roaming“ soll sauber funktionieren
- Monitoring der Netzwerkinfrastruktur erwünscht
- Sicherheit soll erhöht werden:
  Firewalling zwischen Netzwerk-Segmenten
- ...

Mehr verfügbare WLAN-Bandbreite

- WLAN Repeater ersetzen durch Access-Points
- Access-Points per Kabel anbinden
  - Vorteil bei PoE-fähigen Geräten:
    Nur ein (dünnes) Kabel muss verlegt werden
    (Ethernet-Kabel)
  - Strom kommt vom PoE-fähigen Switch
    oder per Injektor

Access-Points statt Repeater



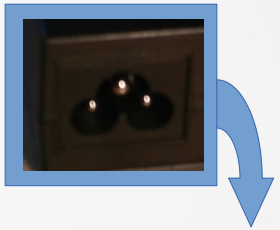
Access-Point

Foto: Bernd Strößenreuther (privat)

Stromversorgung per PoE

Stromversorgung: PoE

PoE-fähiger Switch



Injektor

Alle Fotos auf dieser Seite: Bernd Strößenreuther (privat)

Controller

- Management aller Netzwerkgeräte über einen gemeinsamen Controller
- z. B. https://www.ui.com/download/unifi/
- Bzw. Debian Repo:

```
~# cat /etc/apt/sources.list.d/100-ubnt-unifi.list
deb https://www.ui.com/downloads/unifi/debian stable ubiquiti
```

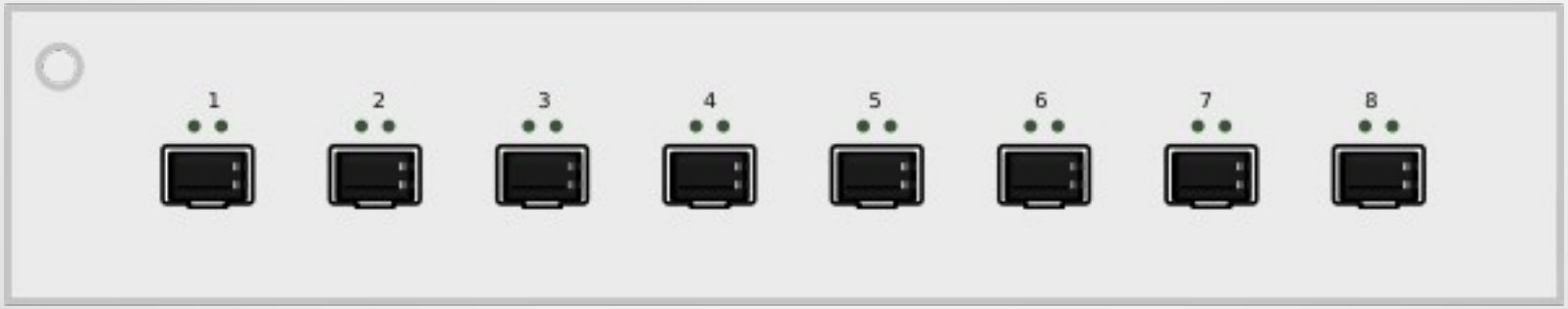
Mehrere Netzwerk-Segmente

- Sicherheit erhöhen
- Zugriffe beschränken für Geräte, denen ggf. nicht vollständig vertraut werden kann
  - Consumer-Geräte, die schon nach relativ kurzer Zeit vom Hersteller keine Sicherheitsupdates mehr erhalten
- Firewall, siehe z. B. https://stroessenreuther.info/pub/Vortrag_Shorewall.pdf
- Brauche ich jetzt für jedes Netzwerk-Segment einen eigenen Switch!?

Exkurs: VLANs

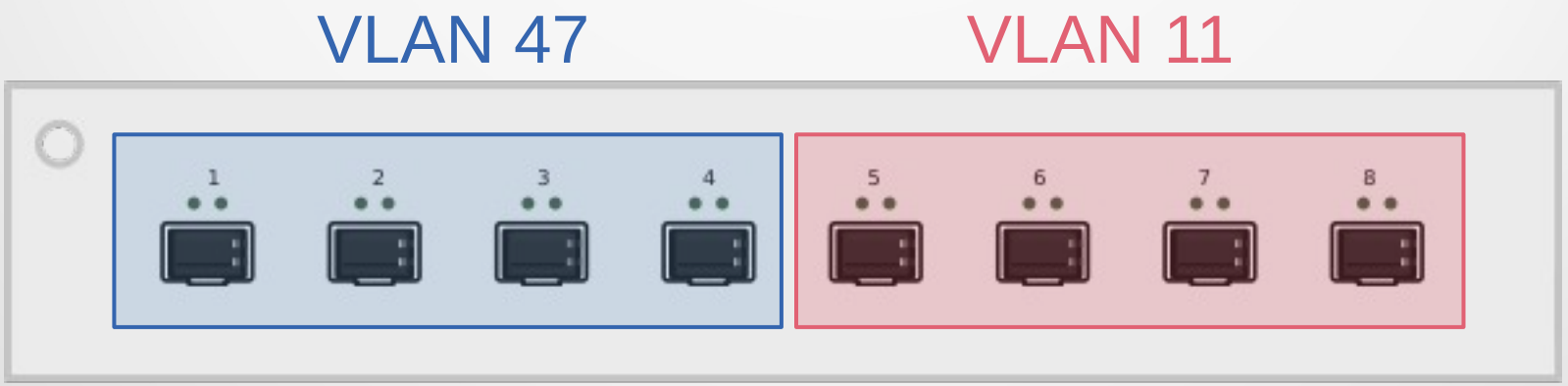
Ohne VLAN:

- Jedes Gerät kann mit jedem beliebigen anderen Gerät direkt sprechen
- Broadcasts erreichen alle anderen Geräte



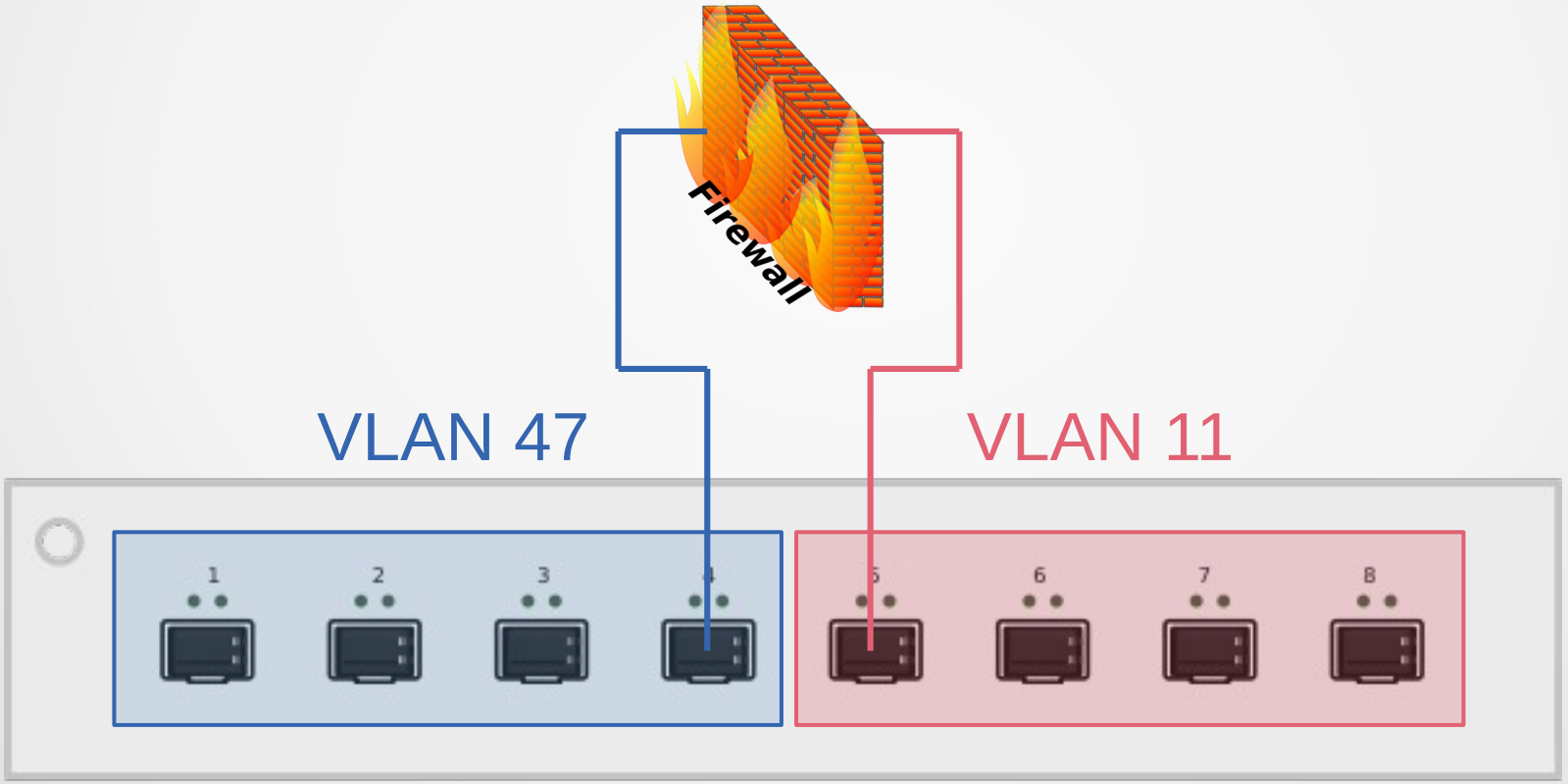
Managementfähiger Switch

- Wir können einen physikalischen Switch aufteilen in mehrere logische Switches
- VLAN 47 ist vollkommen isoliert von VLAN 11 (wie wenn wir 2 physikalische Switches hätten)



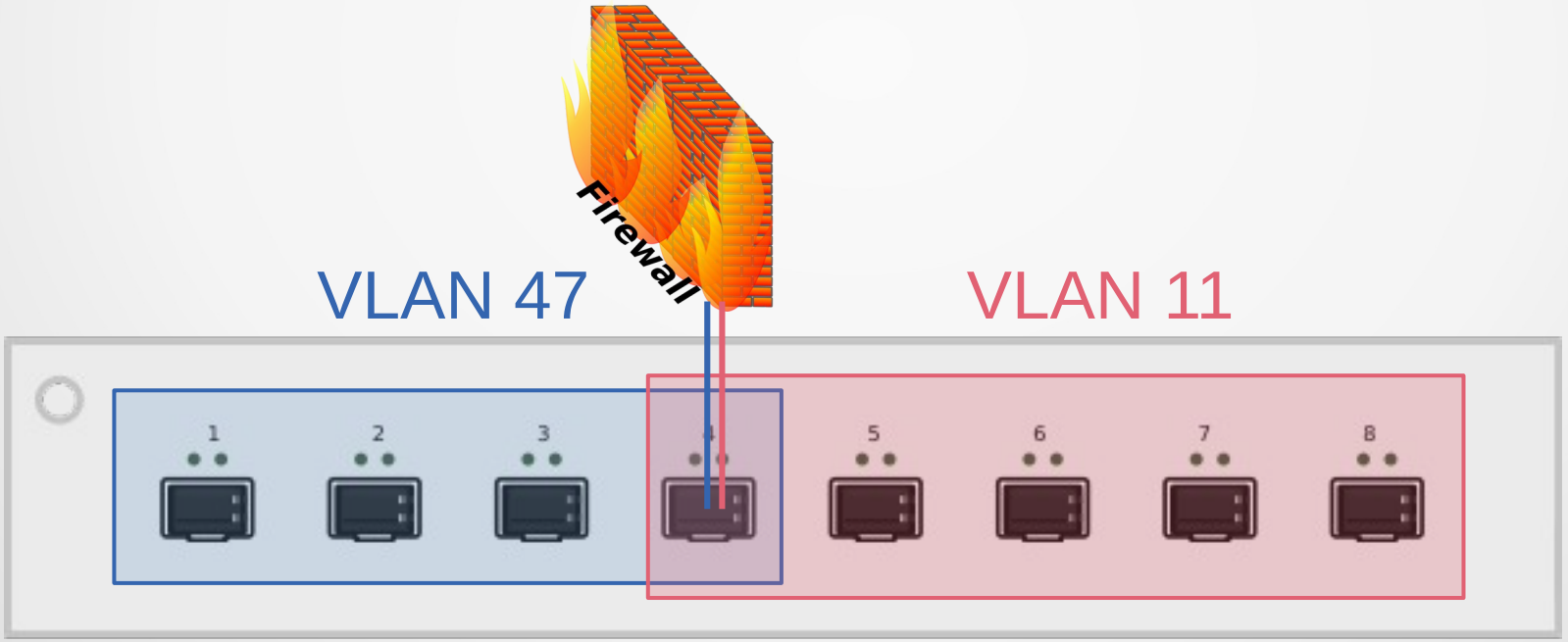
Bestimmte Verbindungen erlauben

Wir packen eine Firewall dazwischen



VLAN Tagging

- Pro Netzwerk-Segment ein physikalischer Port an der Firewall plus ein physikalischer Port am Switch?
- Ist doch irgendwie auch blöd. Warum das nicht auch gleich virtuell?



VLAN Tagging unter Linux

- Die Firewall muss die beiden (logischen) Interfaces trotzdem unterscheiden
- Siehe z. B. https://wiki.ubuntu.com/vlan

cat /etc/network/interfaces

```
# VLAN 47
auto eth2.47
iface eth2.47 inet static
    address 192.168.47.1
    netmask 255.255.255.0
    vlan-raw-device eth2
iface eth2.47 inet6 static
    address 2001:db8:47::1
    netmask 64
    accept_ra 0
```

```
# VLAN 11
auto eth2.11
iface eth2.11 inet static
    address 192.168.11.1
    netmask 255.255.255.0
    vlan-raw-device eth2
iface eth2.11 inet6 static
    address 2001:db8:11::1
    netmask 64
    accept_ra 0
```

~# ifconfig eth2.47

```
eth2.47   Link encap:Ethernet  HWaddr 64:de:ad:be:ef:64
          inet addr:192.168.47.1  Bcast:192.168.47.255  Mask:255.255.255.0
          inet6 addr: 2001:db8:47::1/64 Scope:Global
          inet6 addr: fe80::dead:beef:fe04:5ec/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:1064039 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1991627 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:225695919 (215.2 MiB)  TX bytes:821533912 (783.4 MiB)
```

Live-Demo

Persönliches Fazit

- User-Anforderungen sind offenbar erfüllt:
  Keine Beschwerden mehr!
- „Roaming“: Geräte wechseln zuverlässig und zügig zwischen Access-Points
- Netzwerk-Zugang für einzelne Geräte sperren: 1 Klick
- Sehr übersichtliche Oberfläche: Netzwerk immer im Blick
- Monitoring der WLAN-Interfaces: Feintuning nötig
- Monitoring der Switch-Ports: Ein Kabelbruch war sehr schnell zu lokalisieren

Exkurs: QR-Code für WLAN-Zugriff

Besucher sollen sich möglichst einfach mit dem Gäste-WLAN verbinden können

```
~# qrencode -o Gallien-Gast.png ↵
   'WIFI:S:Gallien-Gast;T:WPA;P:DieSpinnenDieRoemer;;'
```

Beschreibung der Felder siehe z. B.
https://github.com/zxing/zxing/wiki/Barcode-Contents#wi-fi-network-config-android-ios-11

Exkurs: QR-Code für WLAN-Zugriff

Besucher sollen sich möglichst einfach mit dem Gäste-WLAN verbinden können

Wie soll die generierte Bilddatei heißen?

```
~# qrencode -o Gallien-Gast.png ↵
   'WIFI:S:Gallien-Gast;T:WPA;P:DieSpinnenDieRoemer;;'
```

WLAN-SSID

Verschlüsselung

WLAN-Passwort (PSK)

Beschreibung der Felder siehe z. B.
https://github.com/zxing/zxing/wiki/Barcode-Contents#wi-fi-network-config-android-ios-11

Noch Fragen?

- Jetzt und hier
- Bei (fast) jedem Linux-Cafe
- Jederzeit auf der Gluga Users Mailingliste, siehe http://mailing.gluga.de/

Und nicht vergessen: „Machen ist wie wollen, nur krasser.“

(Twitter: @ungehalten)