Technische Hintergründe zum Netzbrief 2014

Von Angriffen, Subnetzen und Layer 3 Switches

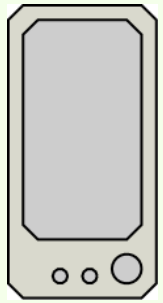
Frank Schiebel, März 2015

Meistens isses doch (im Moment noch) so...

Verwaltungsnetz

Sekretariat, Schulverwaltung
Verbunden mit dem Intranet der Kultusverwaltung

Verwaltungsserver

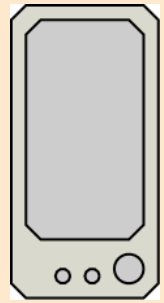


Pädagogisches Netz „Schulnetz“

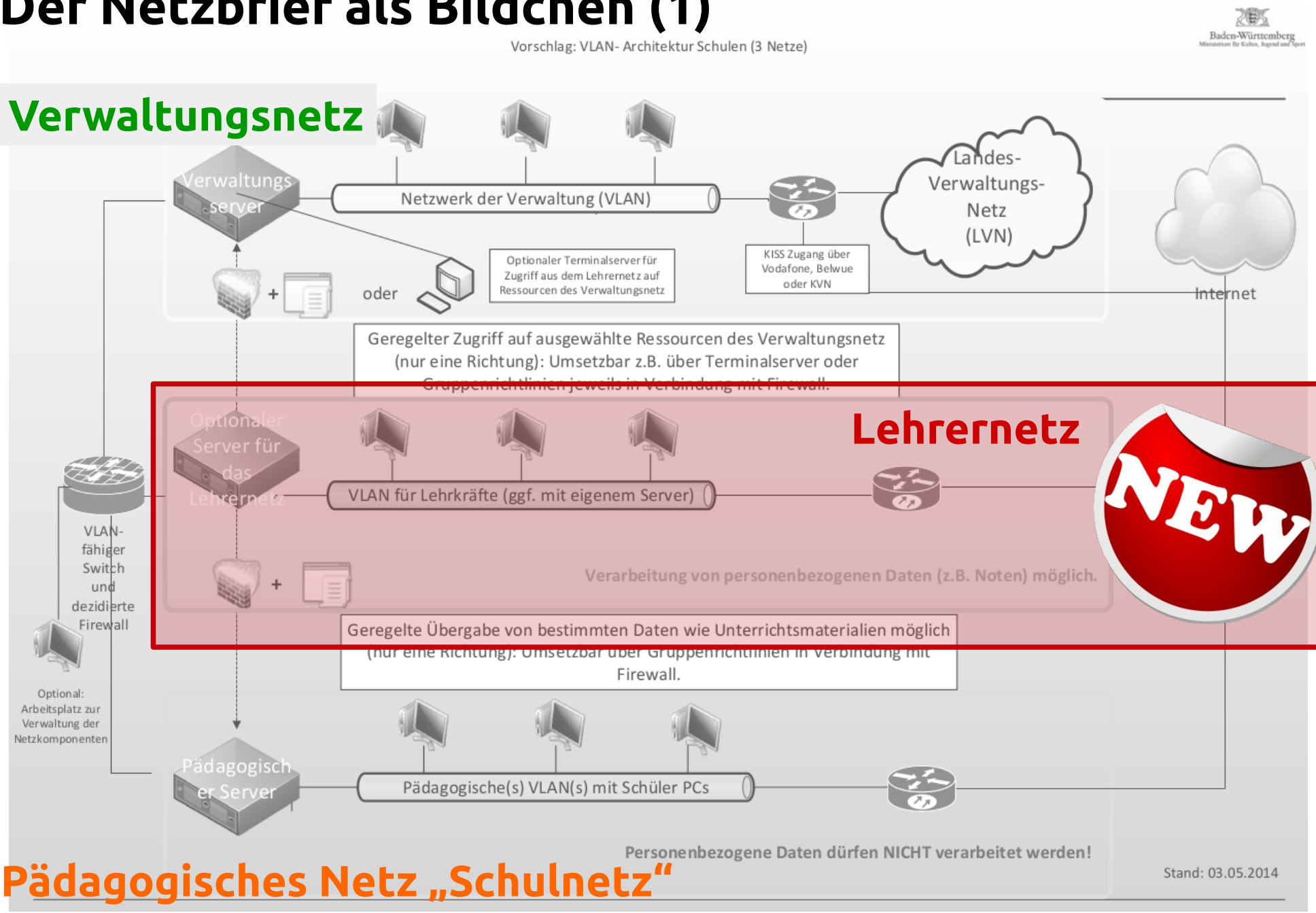
Computerräume
Klassenzimmer
Medienecke
WiFi: Lehrer & Schüler (?)
Lehrerzimmer

Problem – wir werden sehen

Schulserver



Der Netzbrief als Bildchen (1)



Der Hase im Pfeffer...

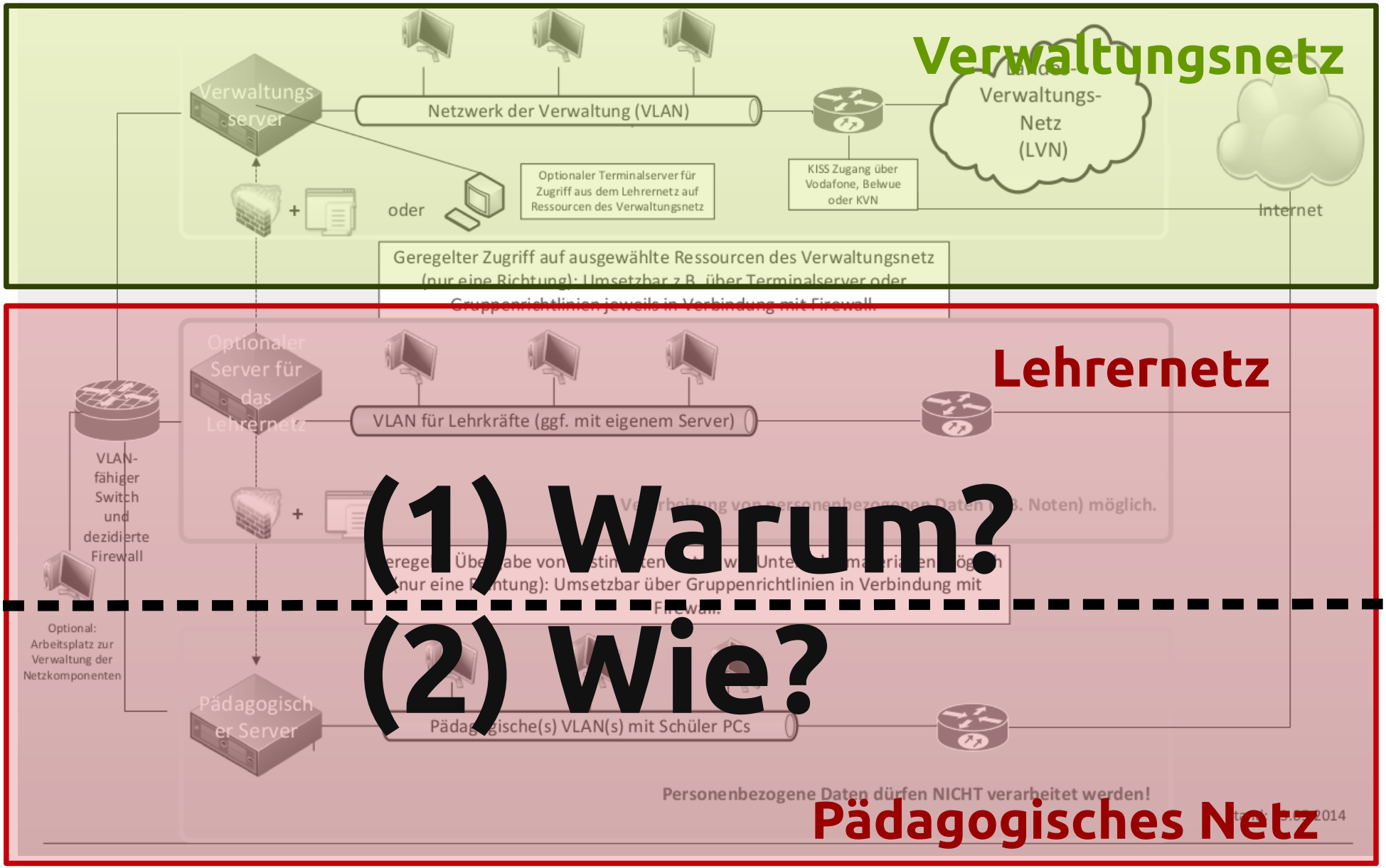
[...]

Vom Lehrernetz aus ist ein geregelter Zugriff in Richtung auf das **Schulverwaltungsnetz** auf ausgewählte Ressourcen zulässig, wenn sichergestellt ist, dass keine personenbezogenen Daten vom Schulverwaltungsnetz dabei im Lehrernetz physikalisch abgelegt werden können.

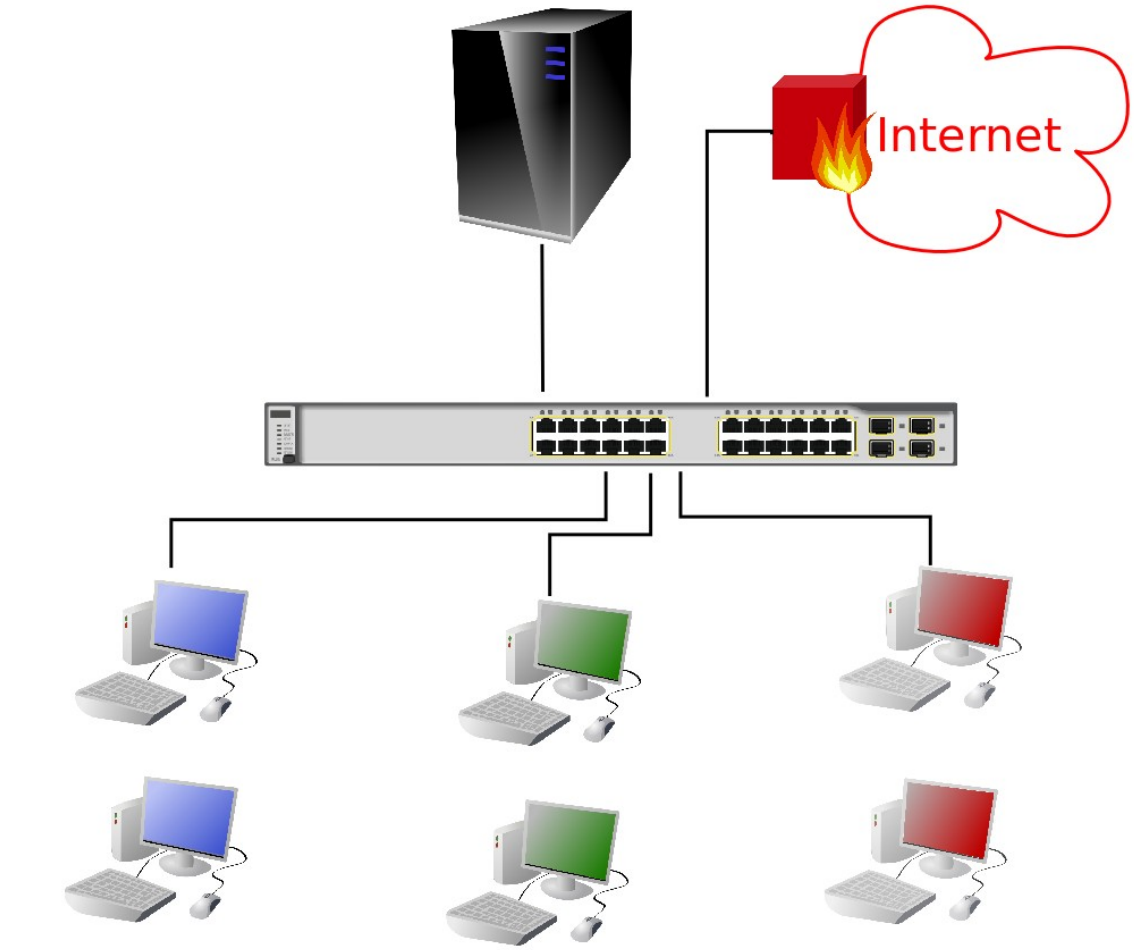
Ein **Zugriff** durch Lehrkräfte vom **Lehrernetz aus auf die Unterrichtsumgebung ist zulässig**. Jeglicher Schülerzugriff auf das Lehrernetz ist unzulässig. Ein Zugriff vom Klassenzimmer aus auf dieses Netz ist zu verhindern.

[...]

Der Netzbrief als Bildchen (2)



Ein besseres Bildchen: Status quo

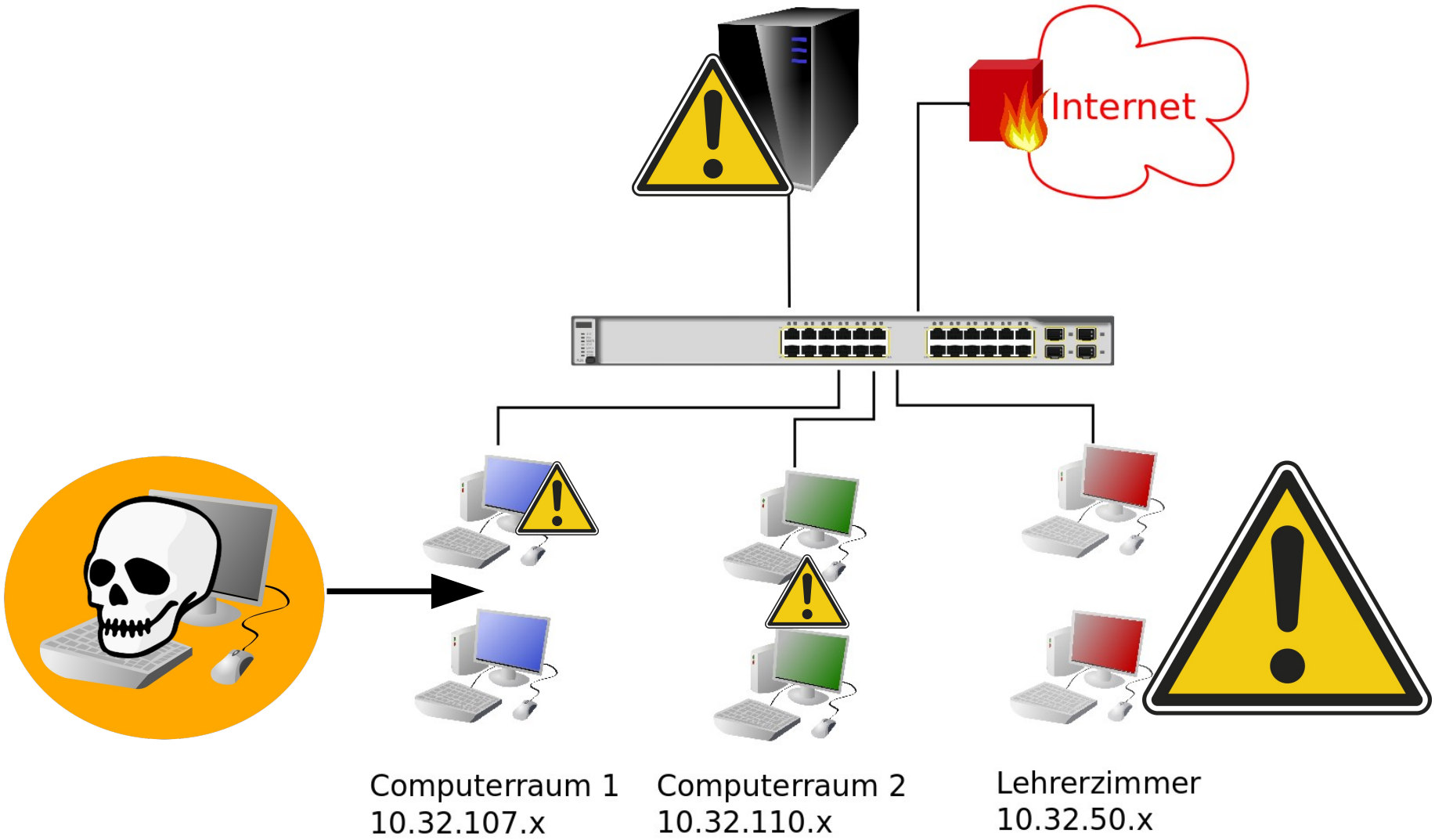


Subnetz: 255.240.0.0
Serveradresse: 10.32.1.1

Alle Rechner befinden sich im selben „Netzsegment“:

```
Address:   10.32.1.1
Netmask:   255.240.0.0 = 12
Wildcard:  0.15.255.255
=>
Network:   10.32.0.0/12
Broadcast: 10.47.255.255
HostMin:   10.32.0.1
HostMax:   10.47.255.254
Hosts/Net: 1048574
```

Der Angreifer

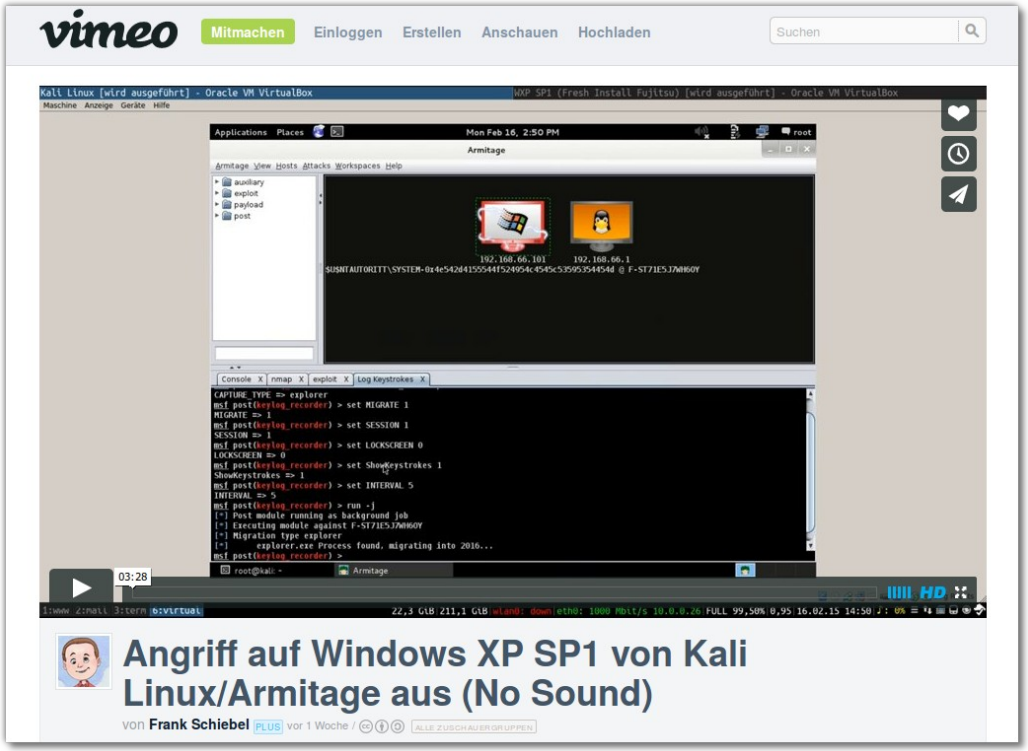


Demo eines Angriffs

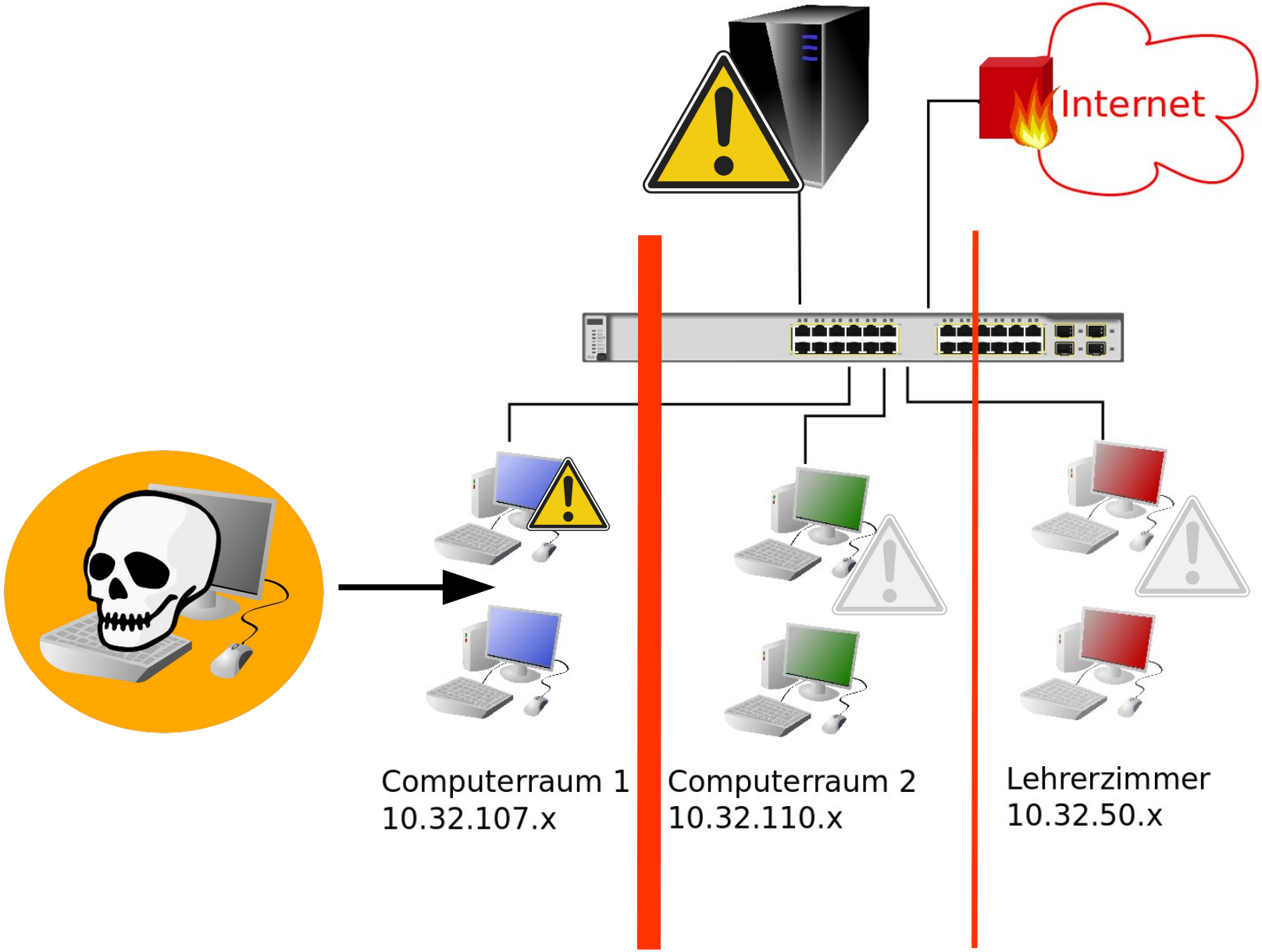
- **Angreifer:** Kali Linux mit Metasploit/Armitage
- **Opfer:** Windows XP SP1 ohne Virenschutz

„Proof of Concept“ → In der Realität evtl. etwas aufwändiger

Zum „Nachschauen“:
https://vimeo.com/119943354



→ Ein Ziel von Subnetting



Wie macht man das? → Die Zutaten...

Layer 3-Switch
(In der Demo ein Cisco SG300-10 ca. 180€)

Muss können... →

IP-basierte Vlans
Routing Funktionalität/ACLs
DHCP Relaying

Idealerweise
Serverlösung, die Subnetting unterstützt
(In der Demo linuxmuster.net 6.1 0€)

Netzkonfiguration für Subnetting

Servernetz
IPs 10.32.1.x
Net 255.255.255.0
GW 10.32.1.253

Firewall: 10.32.1.254

Computerraum 1
IPs 10.32.107.x
Net 255.255.255.0
GW 10.32.107.254

Computerraum 2
IPs 10.32.110.x
Net 255.255.255.0
GW 10.32.110.254

Lehrerzimmer
IPs 10.32.50.x
Net 255.255.255.0
GW 10.32.50.254

Frank Schiebel - frank@linuxmuster.net 03/2015

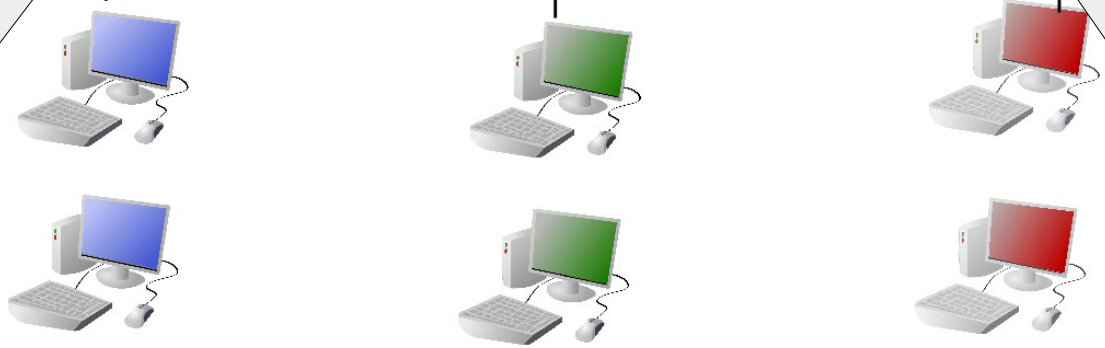
Netzkonfiguration für Subnetting

Servernetz
IPs 10.32.1.x
Net 255.255.255.0
GW 10.32.1.253

Firewall: 10.32.1.254

Server (DHCP) muss „wissen“,
wo anfragender Rechner „steht“

Switch ist Schaltzentrale:
Dient als GW für jedes Subnetz



Computerraum 1
IPs 10.32.107.x
Net 255.255.255.0
GW 10.32.107.254

Computerraum 2
IPs 10.32.110.x
Net 255.255.255.0
GW 10.32.110.254

Lehrerzimmer
IPs 10.32.50.x
Net 255.255.255.0
GW 10.32.50.254

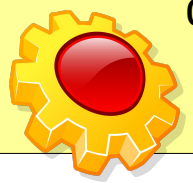
Netzkonfiguration für Subnetting → IP-Adressen

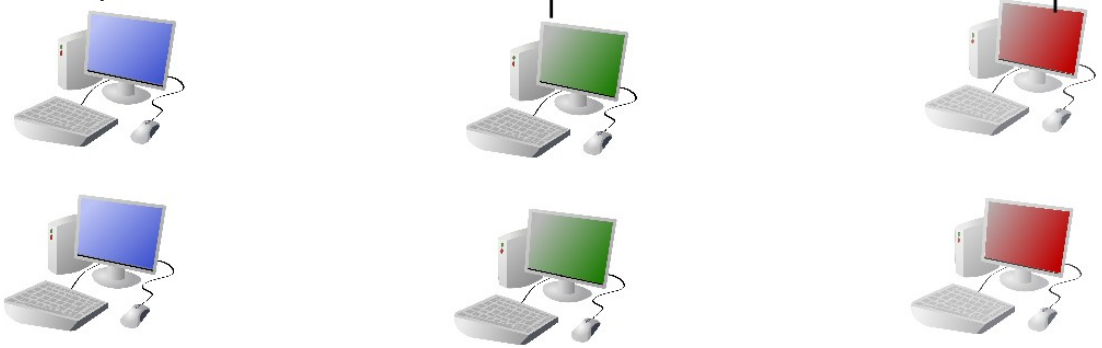
Servernetz
IPs 10.32.1.x
Net 255.255.255.0
GW 10.32.1.253

Firewall: 10.32.1.254

Switch hat eine IP in jedem Subnetz:
10.32.107.254
10.32.110.254
10.32.50.254
10.32.1.253

Jetzt! Switch hat die Kontrolle!



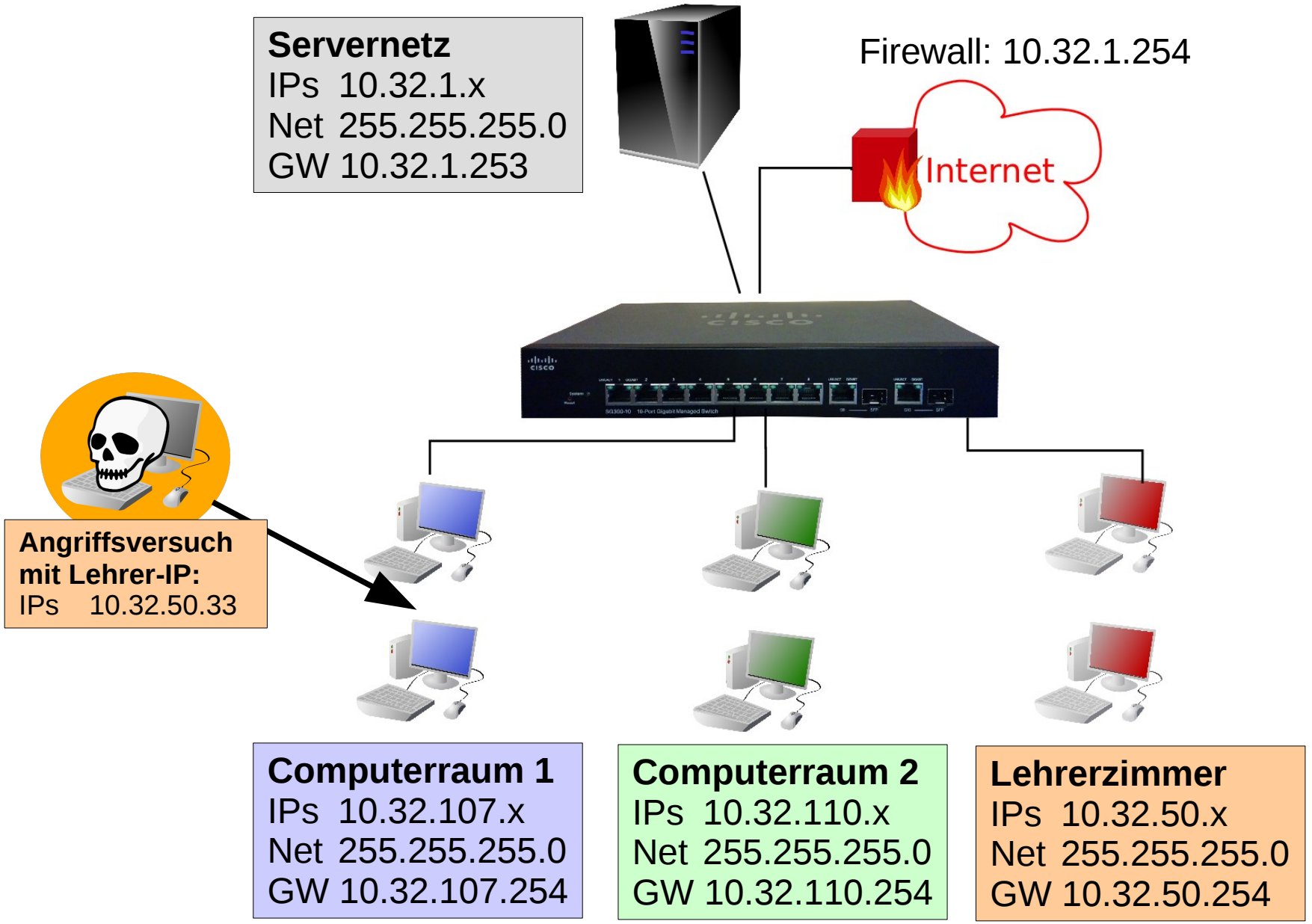


Computerraum 1
IPs 10.32.107.x
Net 255.255.255.0
GW 10.32.107.254

Computerraum 2
IPs 10.32.110.x
Net 255.255.255.0
GW 10.32.110.254

Lehrerzimmer
IPs 10.32.50.x
Net 255.255.255.0
GW 10.32.50.254

Netzkonfiguration für Subnetting → VLANs



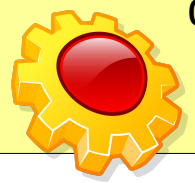
Netzkonfiguration für Subnetting → Ports und ACLs

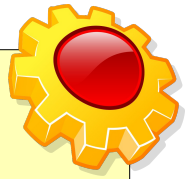
Servernetz
IPs 10.32.1.x
Net 255.255.255.0
GW 10.32.1.253

Firewall: 10.32.1.254

Switch hat eine IP in jedem Subnetz:
VLAN 107 → 10.32.107.254
VLAN 110 → 10.32.110.254
VLAN 50 → 10.32.50.254
VLAN11 → 10.32.1.253

Jetzt! Switch hat die Kontrolle!





IPs werden an VLANs gebunden

VLANs werden an Ports gebunden

Der Übergang wird durch ACLs geregelt

Computerraum 1
IPs 10.32.107.x
Net 255.255.255.0
GW 10.32.107.254

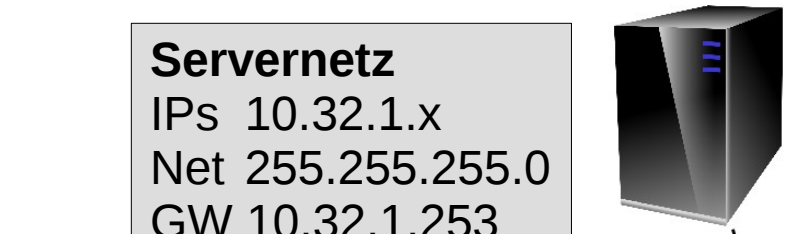
Computerraum 2
IPs 10.32.110.x
Net 255.255.255.0
GW 10.32.110.254

Lehrerzimmer
IPs 10.32.50.x
Net 255.255.255.0
GW 10.32.50.254

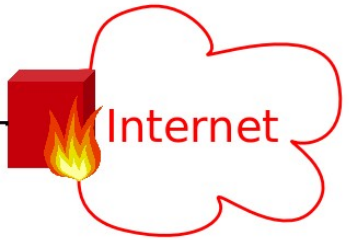
Frank Schiebel - frank@linuxmuster.net 03/2015

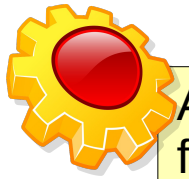
Netzkonfiguration für Subnetting → Ports und ACLs

Servernetz
IPs 10.32.1.x
Net 255.255.255.0
GW 10.32.1.253



Firewall: 10.32.1.254





An diesem **Port** nur Pakete für **VLAN** 107, also mit IP Adressen aus 10.32.107.x

Angriffsversuch mit Lehrer-IP:
IPs 10.32.50.33

Computerraum 1
IPs 10.32.107.x
Net 255.255.255.0
GW 10.32.107.254

Computerraum 2
IPs 10.32.110.x
Net 255.255.255.0
GW 10.32.110.254

Lehrerzimmer
IPs 10.32.50.x
Net 255.255.255.0
GW 10.32.50.254

Probleme und Lösungen

Servernetz
IPs 10.32.1.x
Net 255.255.255.0
GW 10.32.1.253

Firewall: 10.32.1.254

DHCP Broadcasts (Layer 2) bleiben am Switch „hängen“
→ DHCP relaying durch den Switch

WakeonLan vom Server an die Clients (Layer 2) bleiben am Switch „hängen“, müssen weitergereicht werden.

Computerraum 1
IPs 10.32.107.x
Net 255.255.255.0
GW 10.32.107.254

Computerraum 2
IPs 10.32.110.x
Net 255.255.255.0
GW 10.32.110.254

Lehrerzimmer
IPs 10.32.50.x
Net 255.255.255.0
GW 10.32.50.254

Frank Schiebel - frank@linuxmuster.net 03/2015

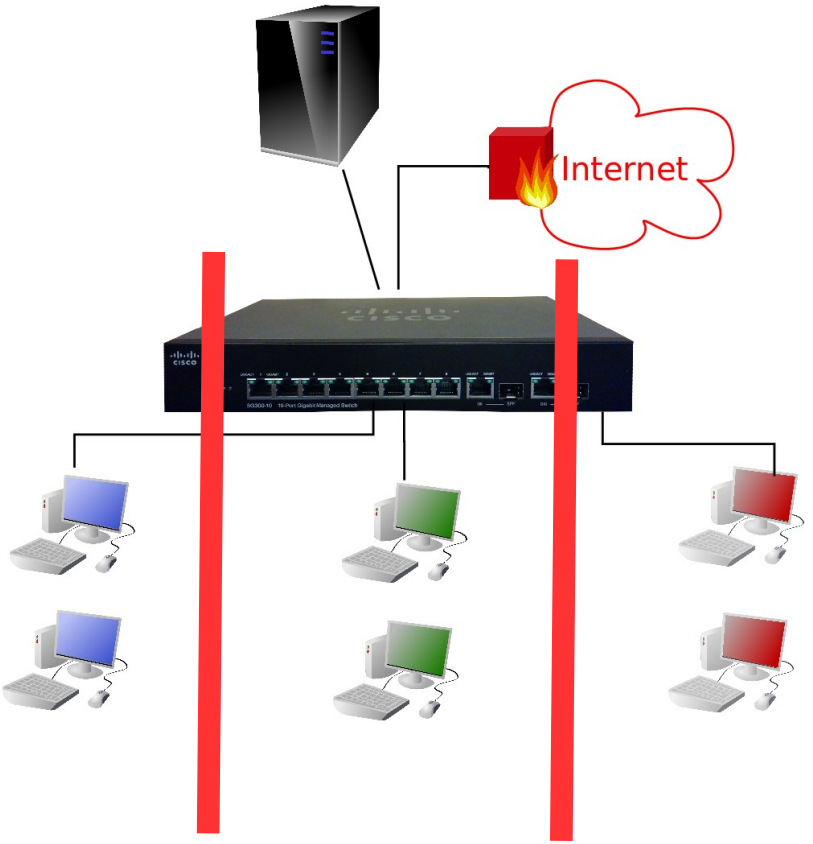
Demo des Netzes mit Subnetting

Rechner aus verschiedenen Subnetzen „sehen“ sich gegenseitig nicht mehr (`ping`)
→ **Angriff schlägt fehl**.

Server ist aus allen Subnetzen erreichbar

Internet ist aus allen Subnetzen **erreichbar**

Je nach Netzsegment erhält ein **neuer** Rechner eine **passende** Adresse



Technik Subnetting: Serverseite

```
13:03/0 server ~ # cat /etc/linuxmuster/subnets
#
# thomas@linuxmuster.net
# 26.11.2013
#
# Example subnet declarations
#
# Network/Prefix ; Router-IP (last IP in network) ; 1. Range-IP ; Last-Range-IP ; Intranet Access 0/1 ; Internet Access 0/1
#
# Servernetz - vlan11 (mit freier Range für Rechneraufnahme)
#10.16.1.0/24;10.16.1.254;10.16.1.100;10.16.1.200;0;0
#
# Lehrernetz - vlan50
10.32.50.0/24;10.32.50.254;10.32.50.100;10.32.50.200;1;1
#
# Raum 107 - vlan107
10.32.107.0/24;10.32.107.254;10.32.107.100;10.32.107.200;1;1
# Raum 110 - vlan110
10.32.110.0/24;10.32.110.254;10.32.110.100;10.32.110.200;1;1
# WLAN BYOD - vlan12
10.32.12.0/24;10.32.12.254;10.32.12.100;10.32.12.200;1;1
# WLAN Lehrer - vlan13
10.32.13.0/24;10.32.13.254;10.32.13.100;10.32.13.200;1;1
```

Subnetze werden in der Datei `/etc/linuxmuster/subnets` definiert (s.o.)

Beim Workstationimport werden die Host DHCP-seitig passend „einsortiert“
→ `import_workstation` erledigt also den Rest „automagisch“

Technik Subnetting: Switch

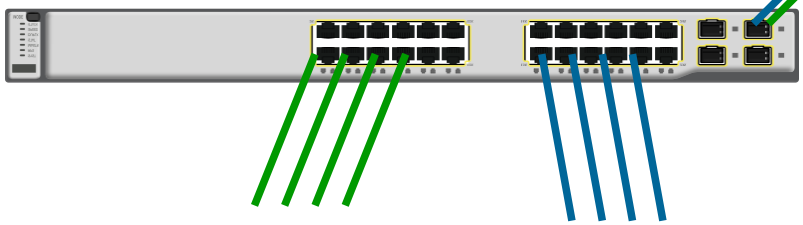
- Für jedes Netzsegment + Servernetz wird ein VLan definiert
- Jedes VLan erhält die passende GW-IP Adresse im Subnetz
- Die Vlans werden getaggt/ungettagt den korrekten Ports zugewiesen
- Es werden ACLs angelegt, die die Kommunikation zwischen den Vlans regeln
- Die Vlan-Konfiguration nachgeordneter (L2-)Switches wird angepasst

Technik Subnetting: Weitere Switchebenen

Layer 2 Switch – muss getaggte Vlans auf L2 verstehen

Port 1:

VLAN 107 (tagged): 10.32.107.254
VLAN 110 (tagged): 10.32.110.254



Ports 1-12 Im VLan 107, Port 12-22 VLan 110
Uplink Port 24 (getaggt) in beiden VLans

Raum 1
10.32.107.x

Raum 2
10.32.110.x

Quellen:

- Netzbrief & Grafik zur *„VLan Architektur (3 Netze)“*: http://www.it.kultus-bw.de/,Lde/Startseite/IT-Sicherheit/Netztechnik+_+Netzbrief
- Diagramme erstellt mit Dia https://wiki.gnome.org/Apps/Dia, Clipart und Grafiken aus den Dia-Objektbögen oder von http://www.openclipart.org
- Dokumentation Subnetting in linuxmuster.net 6.1: http://www.linuxmuster.net/wiki/dokumentation:addons:subnetting:start

- Dieses Dokument steht unter der CC Lizenz *„Namensnennung/Weitergabe unter gleichen Bedingungen 3.0“.* Es darf also (fast) nach belieben verändert und verwendet werden, jedoch muss der Name des ursprünglichen Autors genannt werden und die Bedingungen für die Weitergabe dürfen nicht geändert werden. **Außerdem darf das linuxmuster.net-Logo im Folienfooter nicht entfernt werden.**
- Diese Präsentation online:

  http://www.slideshare.net/ironiemix/subnetting-mit-linuxmusternet-netzbrief-baden-wrttemberg

  (→ http://slidesha.re/1aIGP7D)