

Pimp up your Heimnetzwerk

Bernhard Trummer

`bernhard.trummer@gmx.at`

(0169 6F2E F5F5 6056 DBB3 3997 8109 513D 3377 83A4)

27. April 2018

- **Heimnetzwerk**
- Eigener Server
- Zugriff von außen
- Eigenes WLAN
- Media Streaming
- Q & A

- Heimnetzwerk
- Eigener Server
- Zugriff von außen
- Eigenes WLAN
- Media Streaming
- Q & A

- Heimnetzwerk
- Eigener Server
- Zugriff von außen
- Eigenes WLAN
- Media Streaming
- Q & A

- Heimnetzwerk
- Eigener Server
- Zugriff von außen
- Eigenes WLAN
- Media Streaming
- Q & A

- Heimnetzwerk
- Eigener Server
- Zugriff von außen
- Eigenes WLAN
- Media Streaming
- Q & A

- Heimnetzwerk
- Eigener Server
- Zugriff von außen
- Eigenes WLAN
- Media Streaming
- Q & A

Worum geht es NICHT?

- OpenWRT
 - IPv6
 - VPN
 - Home Automation (z.B. Homematic)
 - IoT

Worum geht es NICHT?

- OpenWRT
- IPv6
- VPN
- Home Automation (z.B. Homematic)
- IoT

Worum geht es NICHT?

- OpenWRT
- IPv6
- VPN
- Home Automation (z.B. Homematic)
- IoT

Worum geht es NICHT?

- OpenWRT
- IPv6
- VPN
- Home Automation (z.B. Homematic)
- IoT

Worum geht es NICHT?

- OpenWRT
- IPv6
- VPN
- Home Automation (z.B. Homematic)
- IoT

- Die dargestellten Konfigurationsbeispiele sind real
- Ähnlichkeiten mit existierenden Heimnetzwerken sind unbeabsichtigt und rein zufällig
- ;-)
- Es geht um mein eigenes Heimnetzwerk
- Und was ich damit mache (bzw. wie)
- Works for me.
- Works for you?

- Die dargestellten Konfigurationsbeispiele sind real
- Ähnlichkeiten mit existierenden Heimnetzwerken sind unbeabsichtigt und rein zufällig
- ;-)
- Es geht um mein eigenes Heimnetzwerk
- Und was ich damit mache (bzw. wie)
- Works for me.
- Works for you?

- Die dargestellten Konfigurationsbeispiele sind real
- Ähnlichkeiten mit existierenden Heimnetzwerken sind unbeabsichtigt und rein zufällig
- ;-)
- Es geht um mein eigenes Heimnetzwerk
- Und was ich damit mache (bzw. wie)
- Works for me.
- Works for you?

- Die dargestellten Konfigurationsbeispiele sind real
- Ähnlichkeiten mit existierenden Heimnetzwerken sind unbeabsichtigt und rein zufällig
- ;-)
- Es geht um mein eigenes Heimnetzwerk
- Und was ich damit mache (bzw. wie)
- Works for me.
- Works for you?

- Die dargestellten Konfigurationsbeispiele sind real
- Ähnlichkeiten mit existierenden Heimnetzwerken sind unbeabsichtigt und rein zufällig
- ;-)
- Es geht um mein eigenes Heimnetzwerk
- Und was ich damit mache (bzw. wie)
- Works for me.
- Works for you?

- Die dargestellten Konfigurationsbeispiele sind real
- Ähnlichkeiten mit existierenden Heimnetzwerken sind unbeabsichtigt und rein zufällig
- ;-)
- Es geht um mein eigenes Heimnetzwerk
- Und was ich damit mache (bzw. wie)
- Works for me.
- Works for you?

- Die dargestellten Konfigurationsbeispiele sind real
- Ähnlichkeiten mit existierenden Heimnetzwerken sind unbeabsichtigt und rein zufällig
- ;-)
- Es geht um mein eigenes Heimnetzwerk
- Und was ich damit mache (bzw. wie)
- Works for me.
- Works for you?

Heimnetzwerk

- Router von Provider (Kabel oder DSL)
- mit WLAN
- PC, Laptop, Handy, Tablet, ...

- Router von Provider (Kabel oder DSL)
- mit WLAN
- PC, Laptop, Handy, Tablet, ...

- Router von Provider (Kabel oder DSL)
- mit WLAN
- PC, Laptop, Handy, Tablet, ...

Verkabelung oder WLAN?

- Warum „oder“, wenn man beides haben kann :-)
- 2x (oder 4x) Cat 6 in jedes Zimmer
- Oder zumindest eine Leerverrohrung
- (wenn die Möglichkeit besteht)

Verkabelung oder WLAN?

- Warum „oder“, wenn man beides haben kann :-)
- 2x (oder 4x) Cat 6 in jedes Zimmer
- Oder zumindest eine Leerverrohrung
- (wenn die Möglichkeit besteht)

Verkabelung oder WLAN?

- Warum „oder“, wenn man beides haben kann :-)
- 2x (oder 4x) Cat 6 in jedes Zimmer
- Oder zumindest eine Leerverrohrung
- (wenn die Möglichkeit besteht)

Verkabelung oder WLAN?

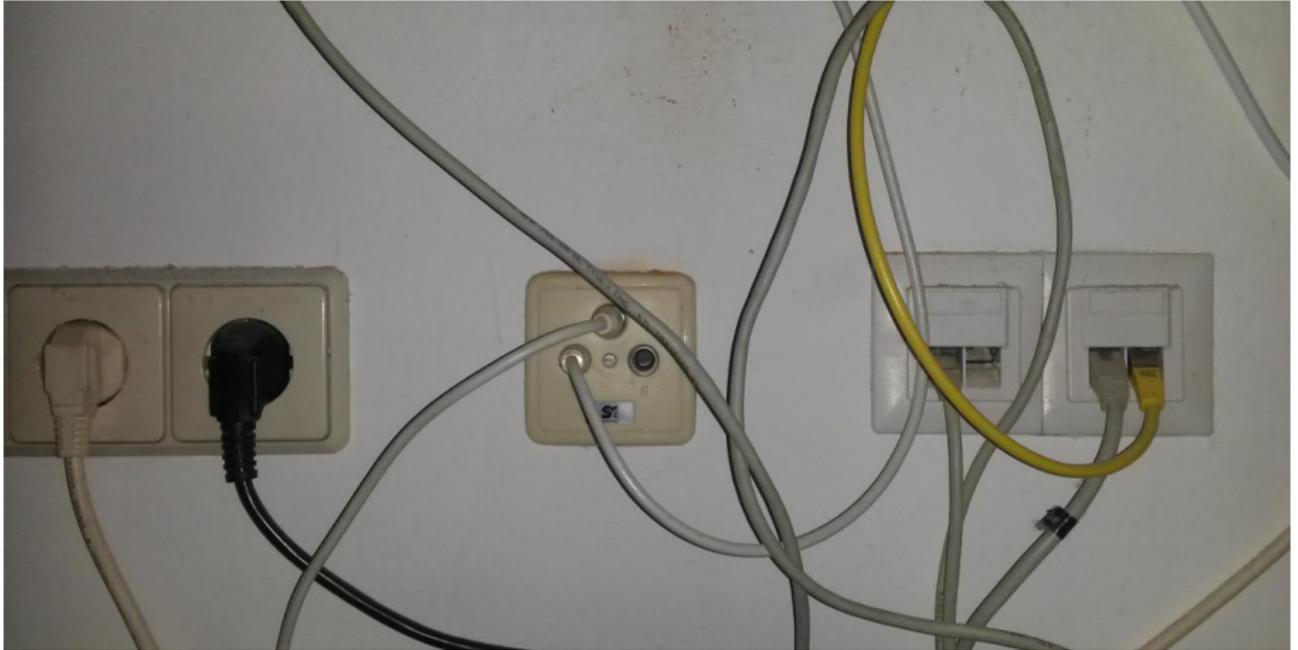
- Warum „oder“, wenn man beides haben kann :-)
- 2x (oder 4x) Cat 6 in jedes Zimmer
- Oder zumindest eine Leerverrohrung
- (wenn die Möglichkeit besteht)

Verkabelung oder WLAN?

- Warum „oder“, wenn man beides haben kann :-)
- 2x (oder 4x) Cat 6 in jedes Zimmer
- Oder zumindest eine Leerverrohrung
- (wenn die Möglichkeit besteht)



Fotos: Wohnzimmer



Eigener Server

- Weil es geht
- Typische Anwendungsfälle:
 - Mediaserver
 - Fileserver bzw. NAS
 - Nextcloud
 - ...

- Weil es geht
- Typische Anwendungsfälle:
 - Mediaserver
 - Fileserver bzw. NAS
 - Nextcloud
 - ...

- Weil es geht
- Typische Anwendungsfälle:
 - Mediaserver
 - Fileserver bzw. NAS
 - Nextcloud
 - ...

- Weil es geht
- Typische Anwendungsfälle:
 - Mediaserver
 - Fileserver bzw. NAS
 - Nextcloud
 - ...

- Weil es geht
- Typische Anwendungsfälle:
 - Mediaserver
 - Fileserver bzw. NAS
 - Nextcloud
 - ...

- Weil es geht
- Typische Anwendungsfälle:
 - Mediaserver
 - Fileserver bzw. NAS
 - Nextcloud
 - ...

Warum???

- Weil es geht
- Unabhängigkeit von „der Cloud“
- Datensparsamkeit
- Weil es Spaß macht
- Weil es sich „richtig“ anfühlt

Warum???

- Weil es geht
- Unabhängigkeit von „der Cloud“
- Datensparsamkeit
- Weil es Spaß macht
- Weil es sich „richtig“ anfühlt

Warum???

- Weil es geht
- Unabhängigkeit von „der Cloud“
- Datensparsamkeit
- Weil es Spaß macht
- Weil es sich „richtig“ anfühlt

Warum???

- Weil es geht
- Unabhängigkeit von „der Cloud“
- Datensparsamkeit
- Weil es Spaß macht
- Weil es sich „richtig“ anfühlt

Warum???

- Weil es geht
- Unabhängigkeit von „der Cloud“
- Datensparsamkeit
- Weil es Spaß macht
- Weil es sich „richtig“ anfühlt

- Kompromiß zwischen Komfort und Privacy
- Verantwortung übernehmen für:
 - Installation / Konfiguration / Betrieb
 - Updates / Patches einspielen
 - Backup / Restore

- Kompromiß zwischen Komfort und Privacy
- Verantwortung übernehmen für:
 - Installation / Konfiguration / Betrieb
 - Updates / Patches einspielen
 - Backup / Restore

- Kompromiß zwischen Komfort und Privacy
- Verantwortung übernehmen für:
 - Installation / Konfiguration / Betrieb
 - Updates / Patches einspielen
 - Backup / Restore

- Kompromiß zwischen Komfort und Privacy
- Verantwortung übernehmen für:
 - Installation / Konfiguration / Betrieb
 - Updates / Patches einspielen
 - Backup / Restore

- Kompromiß zwischen Komfort und Privacy
- Verantwortung übernehmen für:
 - Installation / Konfiguration / Betrieb
 - Updates / Patches einspielen
 - Backup / Restore

- Preis / Leistung / Ausstattung
- Erweiterbarkeit: PCIe, (m)SATA, USB, ...
- Für Dauerbetrieb ausgelegt?
- Bewegliche Teile? (HDD, Lüfter)
- Läuft ein „normales“ Linux drauf?
- Stromverbrauch?

- Preis / Leistung / Ausstattung
- Erweiterbarkeit: PCIe, (m)SATA, USB, ...
- Für Dauerbetrieb ausgelegt?
- Bewegliche Teile? (HDD, Lüfter)
- Läuft ein „normales“ Linux drauf?
- Stromverbrauch?

- Preis / Leistung / Ausstattung
- Erweiterbarkeit: PCIe, (m)SATA, USB, ...
- Für Dauerbetrieb ausgelegt?
- Bewegliche Teile? (HDD, Lüfter)
- Läuft ein „normales“ Linux drauf?
- Stromverbrauch?

- Preis / Leistung / Ausstattung
- Erweiterbarkeit: PCIe, (m)SATA, USB, ...
- Für Dauerbetrieb ausgelegt?
- Bewegliche Teile? (HDD, Lüfter)
- Läuft ein „normales“ Linux drauf?
- Stromverbrauch?

- Preis / Leistung / Ausstattung
- Erweiterbarkeit: PCIe, (m)SATA, USB, ...
- Für Dauerbetrieb ausgelegt?
- Bewegliche Teile? (HDD, Lüfter)
- Läuft ein „normales“ Linux drauf?
- Stromverbrauch?

- Preis / Leistung / Ausstattung
- Erweiterbarkeit: PCIe, (m)SATA, USB, ...
- Für Dauerbetrieb ausgelegt?
- Bewegliche Teile? (HDD, Lüfter)
- Läuft ein „normales“ Linux drauf?
- Stromverbrauch?

- Ein alter PC
- NAS Systeme
- Mini-Computer
 - Raspberry Pi
 - Soekris (net6501)
 - PC Engines (APU)
 - ...

- Ein alter PC
- NAS Systeme
- Mini-Computer
 - Raspberry Pi
 - Soekris (net6501)
 - PC Engines (APU)
 - ...

- Ein alter PC
- NAS Systeme
- Mini-Computer
 - Raspberry Pi
 - Soekris (net6501)
 - PC Engines (APU)
 - ...

- Ein alter PC
- NAS Systeme
- Mini-Computer
 - Raspberry Pi
 - Soekris (net6501)
 - PC Engines (APU)
 - ...

- Ein alter PC
- NAS Systeme
- Mini-Computer
 - Raspberry Pi
 - Soekris (net6501)
 - PC Engines (APU)
 - ...

- Ein alter PC
- NAS Systeme
- Mini-Computer
 - Raspberry Pi
 - Soekris (net6501)
 - PC Engines (APU)
 - ...

- Ein alter PC
- NAS Systeme
- Mini-Computer
 - Raspberry Pi
 - Soekris (net6501)
 - PC Engines (APU)
 - ...

- Soekris net6501
- 250GB SSD (mSATA)
- PCIe-Karte mit 2 zusätzlichen Ethernet-Ports
- WLAN Stick (USB)

- Soekris net6501
- 250GB SSD (mSATA)
- PCIe-Karte mit 2 zusätzlichen Ethernet-Ports
- WLAN Stick (USB)

- Soekris net6501
- 250GB SSD (mSATA)
- PCIe-Karte mit 2 zusätzlichen Ethernet-Ports
- WLAN Stick (USB)

- Soekris net6501
- 250GB SSD (mSATA)
- PCIe-Karte mit 2 zusätzlichen Ethernet-Ports
- WLAN Stick (USB)

Fritz!Box und Soekris



Fritz!Box und Soekris



Grundlegendes Setup (Debian)

- Netzwerk
- NAT
- DHCP Server (isc-dhcp-server)

Grundlegendes Setup (Debian)

- Netzwerk
- NAT
- DHCP Server (isc-dhcp-server)

Grundlegendes Setup (Debian)

- Netzwerk
- NAT
- DHCP Server (isc-dhcp-server)

```
auto lo
iface lo inet loopback

allow-hotplug eth0
iface eth0 inet dhcp

auto eth1
iface eth1 inet static
    address 192.168.1.1
    netmask 255.255.255.0
    network 192.168.1.0
    broadcast 192.168.1.255

# eth2, eth3, ...
```

```
net.ipv4.ip_forward=1
```

```
#!/bin/sh

# Only run for uplink interface.
if [ "$IFACE" != "eth0" ]; then
    exit 0
fi

# Only run from ifup.
if [ "$MODE" != "start" ]; then
    exit 0
fi

...
```

...

```
# Remove any existing rules from all chains
```

```
iptables -F
```

```
iptables -F -t nat
```

```
# Remove any pre-existing user-defined chains
```

```
iptables -X
```

```
iptables -X -t nat
```

```
# Zero counts
```

```
iptables -Z
```

...

```
iptables -t nat -A POSTROUTING -o $IFACE -j MASQUERADE
```

```
default-lease-time 86400;
max-lease-time 86400;

# eth1
subnet 192.168.1.0 netmask 255.255.255.0 {
    range 192.168.1.128 192.168.1.254;
    option routers 192.168.1.1;
    option broadcast-address 192.168.1.255;
}

# eth2, eth3, ...
```

```
host raspberry2 {  
    hardware ethernet b8:27:eb:b4:88:d3;  
    fixed-address 192.168.3.14;  
}
```

...

Zugriff von außen

- Weil es geht
- Fernwartung (SSH)
- Nextcloud für unterwegs (oder für andere)
- ...
- Unabhängigkeit von „der Cloud“

- Weil es geht
- Fernwartung (SSH)
- Nextcloud für unterwegs (oder für andere)
- ...
- Unabhängigkeit von „der Cloud“

- Weil es geht
- Fernwartung (SSH)
- Nextcloud für unterwegs (oder für andere)
- ...
- Unabhängigkeit von „der Cloud“

- Weil es geht
- Fernwartung (SSH)
- Nextcloud für unterwegs (oder für andere)
- ...
- Unabhängigkeit von „der Cloud“

- Weil es geht
- Fernwartung (SSH)
- Nextcloud für unterwegs (oder für andere)
- ...
- Unabhängigkeit von „der Cloud“

Wie funktioniert es?

- Router macht üblicherweise NAT
- D.h. kein „direkter“ Zugriff auf Geräte hinter dem Router
- Die meisten Router können aber „Port Forwarding“
- Oder auch: „Exposed Host“
- Zugriff über öffentliche IP Adresse (des Routers)
- Oder über DNS (eigene Domain oder „Dynamic DNS“)

Wie funktioniert es?

- Router macht üblicherweise NAT
- D.h. kein „direkter“ Zugriff auf Geräte hinter dem Router
- Die meisten Router können aber „Port Forwarding“
- Oder auch: „Exposed Host“
- Zugriff über öffentliche IP Adresse (des Routers)
- Oder über DNS (eigene Domain oder „Dynamic DNS“)

Wie funktioniert es?

- Router macht üblicherweise NAT
- D.h. kein „direkter“ Zugriff auf Geräte hinter dem Router
- Die meisten Router können aber „Port Forwarding“
- Oder auch: „Exposed Host“
- Zugriff über öffentliche IP Adresse (des Routers)
- Oder über DNS (eigene Domain oder „Dynamic DNS“)

Wie funktioniert es?

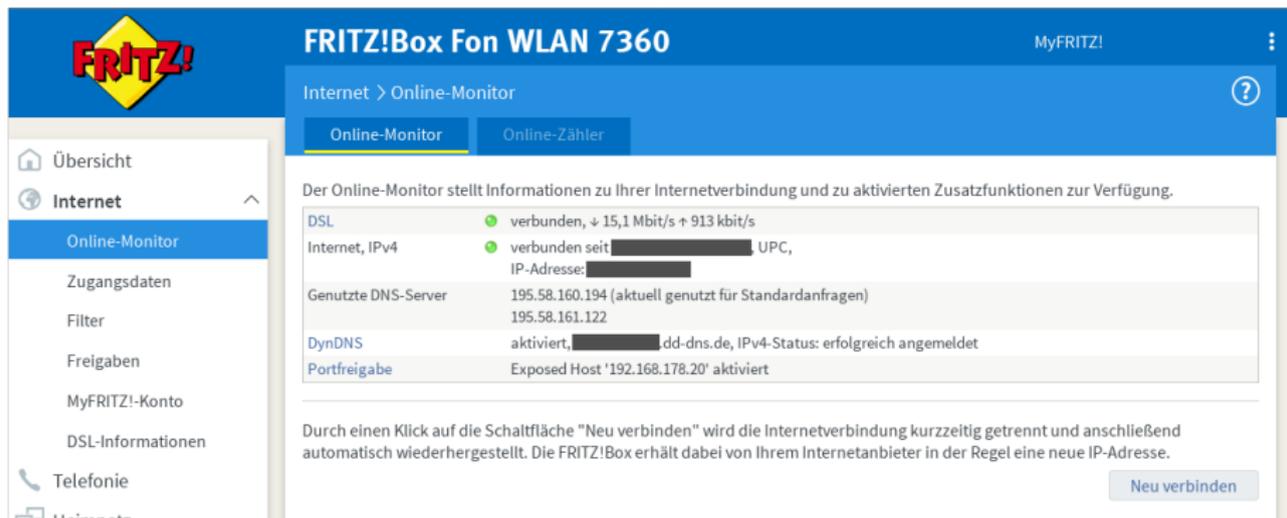
- Router macht üblicherweise NAT
- D.h. kein „direkter“ Zugriff auf Geräte hinter dem Router
- Die meisten Router können aber „Port Forwarding“
- Oder auch: „Exposed Host“
- Zugriff über öffentliche IP Adresse (des Routers)
- Oder über DNS (eigene Domain oder „Dynamic DNS“)

Wie funktioniert es?

- Router macht üblicherweise NAT
- D.h. kein „direkter“ Zugriff auf Geräte hinter dem Router
- Die meisten Router können aber „Port Forwarding“
- Oder auch: „Exposed Host“
- Zugriff über öffentliche IP Adresse (des Routers)
- Oder über DNS (eigene Domain oder „Dynamic DNS“)

Wie funktioniert es?

- Router macht üblicherweise NAT
- D.h. kein „direkter“ Zugriff auf Geräte hinter dem Router
- Die meisten Router können aber „Port Forwarding“
- Oder auch: „Exposed Host“
- Zugriff über öffentliche IP Adresse (des Routers)
- Oder über DNS (eigene Domain oder „Dynamic DNS“)



The screenshot shows the web interface of a Fritz!Box Fon WLAN 7360. The top navigation bar is blue with the Fritz! logo on the left, the device name 'FRITZ!Box Fon WLAN 7360' in the center, and 'MyFRITZ!' on the right. Below the navigation bar, there is a breadcrumb trail 'Internet > Online-Monitor' and a help icon. Two tabs are visible: 'Online-Monitor' (active) and 'Online-Zähler'. The main content area contains a descriptive paragraph and a table of connection details.

FRITZ!Box Fon WLAN 7360 MyFRITZ!

Internet > Online-Monitor

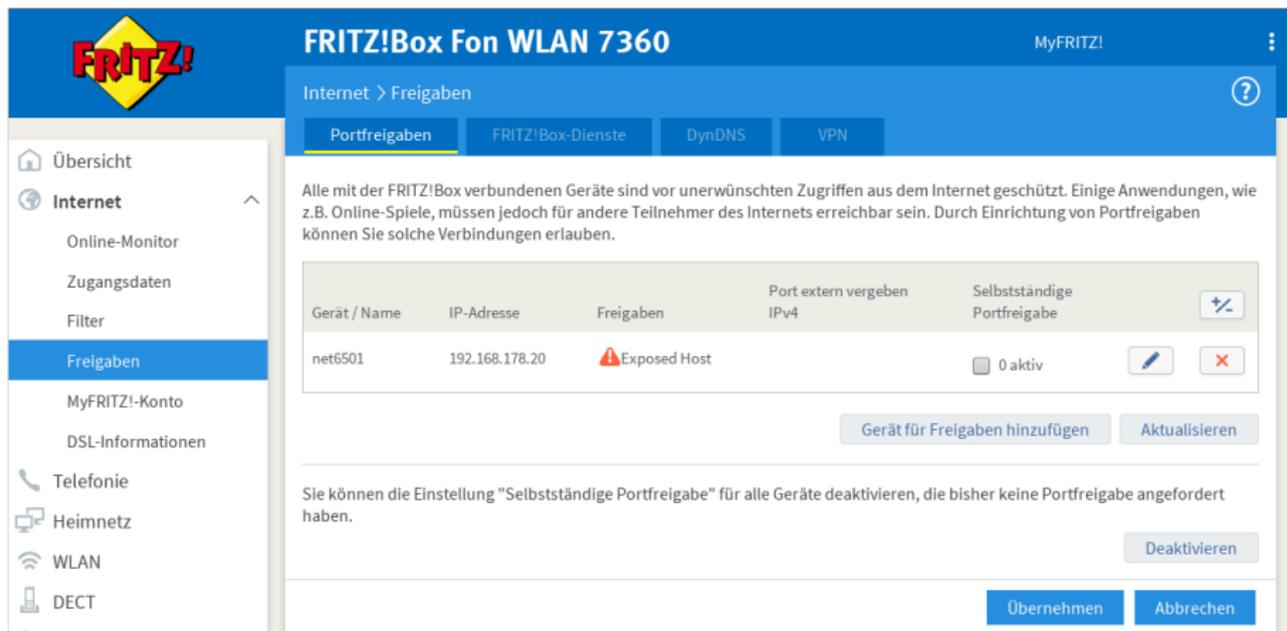
Online-Monitor Online-Zähler

Der Online-Monitor stellt Informationen zu Ihrer Internetverbindung und zu aktivierten Zusatzfunktionen zur Verfügung.

DSL	verbunden, ↓ 15,1 Mbit/s ↑ 913 kbit/s
Internet, IPv4	verbunden seit [redacted] UPC, IP-Adresse: [redacted]
Genutzte DNS-Server	195.58.160.194 (aktuell genutzt für Standardanfragen) 195.58.161.122
DynDNS	aktiviert, [redacted]-dd-dns.de, IPv4-Status: erfolgreich angemeldet
Portfreigabe	Exposed Host '192.168.178.20' aktiviert

Durch einen Klick auf die Schaltfläche "Neu verbinden" wird die Internetverbindung kurzzeitig getrennt und anschließend automatisch wiederhergestellt. Die FRITZ!Box erhält dabei von Ihrem Internetanbieter in der Regel eine neue IP-Adresse.

Neu verbinden



The screenshot shows the Fritz!Box web interface for a FRITZ!Box Fon WLAN 7360. The page is titled "Internet > Freigaben" (Port Forwarding). The left sidebar contains navigation options: Übersicht, Internet (selected), Online-Monitor, Zugangsdaten, Filter, Freigaben (highlighted), MyFRITZ!-Konto, DSL-Informationen, Telefonie, Heimnetz, WLAN, and DECT. The main content area has tabs for "Portfreigaben", "FRITZ!Box-Dienste", "DynDNS", and "VPN". A warning message states: "Alle mit der FRITZ!Box verbundenen Geräte sind vor unerwünschten Zugriffen aus dem Internet geschützt. Einige Anwendungen, wie z.B. Online-Spiele, müssen jedoch für andere Teilnehmer des Internets erreichbar sein. Durch Einrichtung von Portfreigaben können Sie solche Verbindungen erlauben." Below this is a table with columns: "Gerät / Name", "IP-Adresse", "Freigaben", "Port extern vergeben IPv4", and "Selbstständige Portfreigabe". One entry is shown: "net6501" with IP "192.168.178.20" and status "Exposed Host". The "Selbstständige Portfreigabe" column shows "0 aktiv". Action buttons include "Gerät für Freigaben hinzufügen", "Aktualisieren", "Deaktivieren", "Übernehmen", and "Abbrechen".

FRITZ!Box Fon WLAN 7360 MyFRITZ!

Internet > Freigaben

Portfreigaben FRITZ!Box-Dienste DynDNS VPN

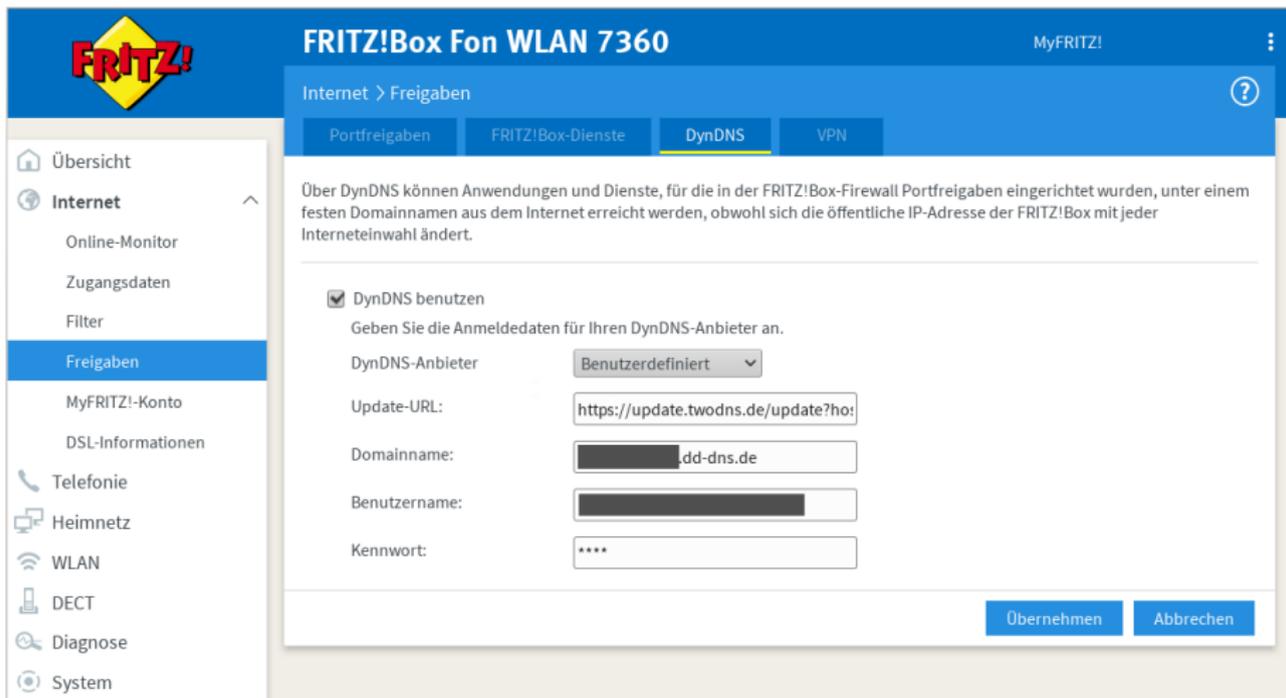
Alle mit der FRITZ!Box verbundenen Geräte sind vor unerwünschten Zugriffen aus dem Internet geschützt. Einige Anwendungen, wie z.B. Online-Spiele, müssen jedoch für andere Teilnehmer des Internets erreichbar sein. Durch Einrichtung von Portfreigaben können Sie solche Verbindungen erlauben.

Gerät / Name	IP-Adresse	Freigaben	Port extern vergeben IPv4	Selbstständige Portfreigabe
net6501	192.168.178.20	⚠ Exposed Host		<input type="checkbox"/> 0 aktiv

[Gerät für Freigaben hinzufügen](#) [Aktualisieren](#)

Sie können die Einstellung "Selbstständige Portfreigabe" für alle Geräte deaktivieren, die bisher keine Portfreigabe angefordert haben. [Deaktivieren](#)

[Übernehmen](#) [Abbrechen](#)



The screenshot shows the web interface of a Fritz!Box Fon WLAN 7360. The top navigation bar is blue with the Fritz! logo on the left, the device name 'FRITZ!Box Fon WLAN 7360' in the center, and 'MyFRITZ!' on the right. Below the navigation bar, there is a breadcrumb trail 'Internet > Freigaben' and a help icon. A secondary navigation bar contains tabs for 'Portfreigaben', 'FRITZ!Box-Dienste', 'DynDNS' (which is selected and underlined), and 'VPN'. The main content area has a heading 'Über DynDNS können Anwendungen und Dienste, für die in der FRITZ!Box-Firewall Portfreigaben eingerichtet wurden, unter einem festen Domainnamen aus dem Internet erreicht werden, obwohl sich die öffentliche IP-Adresse der FRITZ!Box mit jeder Interneteinwahl ändert.' Below this, there is a checkbox 'DynDNS benutzen' which is checked. A sub-heading reads 'Geben Sie die Anmeldedaten für Ihren DynDNS-Anbieter an.' The form contains the following fields: 'DynDNS-Anbieter' (a dropdown menu set to 'Benutzerdefiniert'), 'Update-URL:' (a text box containing 'https://update.twodns.de/update?ho:'), 'Domainname:' (a text box containing a redacted domain followed by '.dd-dns.de'), 'Benutzername:' (a text box with a redacted username), and 'Kennwort:' (a password field with four asterisks). At the bottom right of the form are two buttons: 'Übernehmen' and 'Abbrechen'. On the left side of the interface is a sidebar menu with icons and labels for 'Übersicht', 'Internet' (selected), 'Online-Monitor', 'Zugangsdaten', 'Filter', 'Freigaben' (highlighted in blue), 'MyFRITZ!-Konto', 'DSL-Informationen', 'Telefonie', 'Heimnetz', 'WLAN', 'DECT', 'Diagnose', and 'System'.

Port Forwardings

```
iptables -t nat -A PREROUTING -i $IFACE \  
-p tcp --dport 12345 -j DNAT --to 192.168.1.42
```

Security Warning!

- Das Internet ist kein Ponyhof
- Dein Server WIRD auf verschiedene Arten angegriffen werden!
- Im Zweifel:
 - Lieber nichts nach außen freigeben
 - Lieber jemanden fragen, der sich auskennt
 - Lesen und lernen

- Das Internet ist kein Ponyhof
- Dein Server WIRD auf verschiedene Arten angegriffen werden!
- Im Zweifel:
 - Lieber nichts nach außen freigeben
 - Lieber jemanden fragen, der sich auskennt
 - Lesen und lernen

- Das Internet ist kein Ponyhof
- Dein Server WIRD auf verschiedene Arten angegriffen werden!
- Im Zweifel:
 - Lieber nichts nach außen freigeben
 - Lieber jemanden fragen, der sich auskennt
 - Lesen und lernen

- Das Internet ist kein Ponyhof
- Dein Server WIRD auf verschiedene Arten angegriffen werden!
- Im Zweifel:
 - Lieber nichts nach außen freigeben
 - Lieber jemanden fragen, der sich auskennt
 - Lesen und lernen

- Das Internet ist kein Ponyhof
- Dein Server WIRD auf verschiedene Arten angegriffen werden!
- Im Zweifel:
 - Lieber nichts nach außen freigeben
 - Lieber jemanden fragen, der sich auskennt
 - Lesen und lernen

- Das Internet ist kein Ponyhof
- Dein Server WIRD auf verschiedene Arten angegriffen werden!
- Im Zweifel:
 - Lieber nichts nach außen freigeben
 - Lieber jemanden fragen, der sich auskennt
 - Lesen und lernen

- SSH
- Apache (TLS)
- Ich habe genau das gemacht
- ... und ich kann nachts ruhig schlafen. :-)

- SSH
- Apache (TLS)
- Ich habe genau das gemacht
- ... und ich kann nachts ruhig schlafen. :-)

- SSH
- Apache (TLS)
- Ich habe genau das gemacht
- ... und ich kann nachts ruhig schlafen. :-)

- Häufig zu sehen: Username/Paßwort Wörterbuch-Attacken
- Gegenmaßnahmen:
 - Kein direktes root-Login erlauben
 - Sichere Paßwörter
 - Standardpaßwörter ändern (pi/raspberry)
 - Oder besser: nur Public-Key Authentifizierung zulassen

- Häufig zu sehen: Username/Paßwort Wörterbuch-Attacken
- Gegenmaßnahmen:
 - Kein direktes root-Login erlauben
 - Sichere Paßwörter
 - Standardpaßwörter ändern (pi/raspberry)
 - Oder besser: nur Public-Key Authentifizierung zulassen

- Häufig zu sehen: Username/Paßwort Wörterbuch-Attacken
- Gegenmaßnahmen:
 - Kein direktes root-Login erlauben
 - Sichere Paßwörter
 - Standardpaßwörter ändern (pi/raspberry)
 - Oder besser: nur Public-Key Authentifizierung zulassen

- Häufig zu sehen: Username/Paßwort Wörterbuch-Attacken
- Gegenmaßnahmen:
 - Kein direktes root-Login erlauben
 - Sichere Paßwörter
 - Standardpaßwörter ändern (pi/raspberry)
 - Oder besser: nur Public-Key Authentifizierung zulassen

- Häufig zu sehen: Username/Paßwort Wörterbuch-Attacken
- Gegenmaßnahmen:
 - Kein direktes root-Login erlauben
 - Sichere Paßwörter
 - Standardpaßwörter ändern (pi/raspberry)
 - Oder besser: nur Public-Key Authentifizierung zulassen

- Häufig zu sehen: Username/Paßwort Wörterbuch-Attacken
- Gegenmaßnahmen:
 - Kein direktes root-Login erlauben
 - Sichere Paßwörter
 - Standardpaßwörter ändern (pi/raspberry)
 - Oder besser: nur Public-Key Authentifizierung zulassen

```
PermitRootLogin no  
StrictModes yes  
AllowUsers slash
```

```
PubkeyAuthentication yes  
PasswordAuthentication no  
PermitEmptyPasswords no  
ChallengeResponseAuthentication no  
KerberosAuthentication no  
GSSAPIAuthentication no
```

Teergrube für eingehende Verbindungen

```
SSH_PORT=22
```

```
iptables -A INPUT -i $IFACE -p tcp --dport ${SSH_PORT} \  
  --syn -m recent --name ssh \  
  --update --seconds 600 --hitcount 5 -j DROP
```

```
iptables -A INPUT -i $IFACE -p tcp --dport ${SSH_PORT} \  
  --syn -m recent --name ssh \  
  --set
```

- <https://www.fail2ban.org/>
- https://www.thomas-krenn.com/de/wiki/SSH_Login_unter_Debian_mit_fail2ban_absichern

- <https://www.fail2ban.org/>
- https://www.thomas-krenn.com/de/wiki/SSH_Login_unter_Debian_mit_fail2ban_absichern

- Spätestens seit Snowden: TLS ist Pflicht!
- TLS schützt aber nur den Transport, nicht den Server
- Starke Paßwörter (z.B. Nextcloud) auch wichtig!
- Woher ein TLS Zertifikat beziehen?

- Spätestens seit Snowden: TLS ist Pflicht!
- TLS schützt aber nur den Transport, nicht den Server
- Starke Paßwörter (z.B. Nextcloud) auch wichtig!
- Woher ein TLS Zertifikat beziehen?

- Spätestens seit Snowden: TLS ist Pflicht!
- TLS schützt aber nur den Transport, nicht den Server
- Starke Paßwörter (z.B. Nextcloud) auch wichtig!
- Woher ein TLS Zertifikat beziehen?

- Spätestens seit Snowden: TLS ist Pflicht!
- TLS schützt aber nur den Transport, nicht den Server
- Starke Paßwörter (z.B. Nextcloud) auch wichtig!
- Woher ein TLS Zertifikat beziehen?

- Offene und freie CA
- Vollautomatisiert:
 - Schlüsselgenerierung
 - Beantragen des Zertifikats
 - (initial oder Erneuerung)
 - Installation in den Webserver
- <https://certbot.eff.org/>

- Offene und freie CA
- Vollautomatisiert:
 - Schlüsselgenerierung
 - Beantragen des Zertifikats
 - (initial oder Erneuerung)
 - Installation in den Webserver
- <https://certbot.eff.org/>

- Offene und freie CA
- Vollautomatisiert:
 - Schlüsselgenerierung
 - Beantragen des Zertifikats
 - (initial oder Erneuerung)
 - Installation in den Webserver
- <https://certbot.eff.org/>

- Offene und freie CA
- Vollautomatisiert:
 - Schlüsselgenerierung
 - Beantragen des Zertifikats
 - (initial oder Erneuerung)
 - Installation in den Webserver
- <https://certbot.eff.org/>

- Offene und freie CA
- Vollautomatisiert:
 - Schlüsselgenerierung
 - Beantragen des Zertifikats
 - (initial oder Erneuerung)
 - Installation in den Webserver
- <https://certbot.eff.org/>

- Offene und freie CA
- Vollautomatisiert:
 - Schlüsselgenerierung
 - Beantragen des Zertifikats
 - (initial oder Erneuerung)
 - Installation in den Webserver
- <https://certbot.eff.org/>

- Offene und freie CA
- Vollautomatisiert:
 - Schlüsselgenerierung
 - Beantragen des Zertifikats
 - (initial oder Erneuerung)
 - Installation in den Webserver
- <https://certbot.eff.org/>

- SSL (auch v3) deaktivieren
- Schwache Ciphers deaktivieren
- Online-Test: <https://www.ssllabs.com/ssltest/>

- SSL (auch v3) deaktivieren
- Schwache Ciphers deaktivieren
- Online-Test: <https://www.ssllabs.com/ssltest/>

- SSL (auch v3) deaktivieren
- Schwache Ciphers deaktivieren
- Online-Test: <https://www.ssllabs.com/ssltest/>

```
<IfModule mod_headers.c>
    Header always set Strict-Transport-Security
        "max-age=15768000; includeSubDomains; preload"
</IfModule>

# Intermediate configuration, tweak to your needs
SSLProtocol          all -SSLv2 -SSLv3 -TLSv1 -TLSv1.1
SSLCipherSuite       HIGH:!aNULL
SSLHonorCipherOrder  on

SSLOptions +StrictRequire
```

Eigenes WLAN

- \$MODEM hat ja eh WLAN dabei
- Ja, eh, aber...

Warum?

- \$MODEM hat ja eh WLAN dabei
- Ja, eh, aber...

- Weil es geht
- Mitschauen, was \$HANDY und \$TV so machen
- Trennung zwischen Gast- und internes WLAN
- Datensparsamkeit für „Smart“ Devices erzwingen:
 - Gezielte DNS Sperren
 - Gezielte Paketfilterung
 - ...

- Weil es geht
- Mitschauen, was \$HANDY und \$TV so machen
- Trennung zwischen Gast- und internes WLAN
- Datensparsamkeit für „Smart“ Devices erzwingen:
 - Gezielte DNS Sperren
 - Gezielte Paketfilterung
 - ...

- Weil es geht
- Mitschauen, was \$HANDY und \$TV so machen
- Trennung zwischen Gast- und internes WLAN
- Datensparsamkeit für „Smart“ Devices erzwingen:
 - Gezielte DNS Sperren
 - Gezielte Paketfilterung
 - ...

- Weil es geht
- Mitschauen, was \$HANDY und \$TV so machen
- Trennung zwischen Gast- und internes WLAN
- Datensparsamkeit für „Smart“ Devices erzwingen:
 - Gezielte DNS Sperren
 - Gezielte Paketfilterung
 - ...

- Weil es geht
- Mitschauen, was \$HANDY und \$TV so machen
- Trennung zwischen Gast- und internes WLAN
- Datensparsamkeit für „Smart“ Devices erzwingen:
 - Gezielte DNS Sperren
 - Gezielte Paketfilterung
 - ...

- Weil es geht
- Mitschauen, was \$HANDY und \$TV so machen
- Trennung zwischen Gast- und internes WLAN
- Datensparsamkeit für „Smart“ Devices erzwingen:
 - Gezielte DNS Sperren
 - Gezielte Paketfilterung
 - ...

- Weil es geht
- Mitschauen, was \$HANDY und \$TV so machen
- Trennung zwischen Gast- und internes WLAN
- Datensparsamkeit für „Smart“ Devices erzwingen:
 - Gezielte DNS Sperren
 - Gezielte Paketfilterung
 - ...

- Hardware
 - WLAN USB-Stick
- Software
 - Firmware für den Chipsatz
 - hostapd

- Hardware
 - WLAN USB-Stick
- Software
 - Firmware für den Chipsatz
 - hostapd

Wie gehts?

- Hardware
 - WLAN USB-Stick
- Software
 - Firmware für den Chipsatz
 - hostapd

Wie gehts?

- Hardware
 - WLAN USB-Stick
- Software
 - Firmware für den Chipsatz
 - hostapd

- Hardware
 - WLAN USB-Stick
- Software
 - Firmware für den Chipsatz
 - hostapd

Hardware: welcher Stick genau?

- https://en.wikipedia.org/wiki/Comparison_of_open-source_wireless_drivers
- Muß „Master (AP) Mode“ unterstützen
- Edimax EW-7612UAn
 - RTL8192cu
 - nicht gut...
 - auch mit Download-Firmware
 - (das war vor ca. drei Jahren...)
- Sticks mit Ralink RT5370 Chipsatz
 - zwar mit non-free Firmware
 - funktioniert aber super!

Hardware: welcher Stick genau?

- https://en.wikipedia.org/wiki/Comparison_of_open-source_wireless_drivers
- Muß „Master (AP) Mode“ unterstützen
- Edimax EW-7612UAn
 - RTL8192cu
 - nicht gut...
 - auch mit Download-Firmware
 - (das war vor ca. drei Jahren...)
- Sticks mit Ralink RT5370 Chipsatz
 - zwar mit non-free Firmware
 - funktioniert aber super!

Hardware: welcher Stick genau?

- https://en.wikipedia.org/wiki/Comparison_of_open-source_wireless_drivers
- Muß „Master (AP) Mode“ unterstützen
- Edimax EW-7612UAn
 - RTL8192cu
 - nicht gut...
 - auch mit Download-Firmware
 - (das war vor ca. drei Jahren...)
- Sticks mit Ralink RT5370 Chipsatz
 - zwar mit non-free Firmware
 - funktioniert aber super!

Hardware: welcher Stick genau?

- https://en.wikipedia.org/wiki/Comparison_of_open-source_wireless_drivers
- Muß „Master (AP) Mode“ unterstützen
- Edimax EW-7612UAn
 - RTL8192cu
 - nicht gut...
 - auch mit Download-Firmware
 - (das war vor ca. drei Jahren...)
- Sticks mit Ralink RT5370 Chipsatz
 - zwar mit non-free Firmware
 - funktioniert aber super!

Hardware: welcher Stick genau?

- https://en.wikipedia.org/wiki/Comparison_of_open-source_wireless_drivers
- Muß „Master (AP) Mode“ unterstützen
- Edimax EW-7612UAn
 - RTL8192cu
 - nicht gut...
 - auch mit Download-Firmware
 - (das war vor ca. drei Jahren...)
- Sticks mit Ralink RT5370 Chipsatz
 - zwar mit non-free Firmware
 - funktioniert aber super!

Hardware: welcher Stick genau?

- https://en.wikipedia.org/wiki/Comparison_of_open-source_wireless_drivers
- Muß „Master (AP) Mode“ unterstützen
- Edimax EW-7612UAn
 - RTL8192cu
 - nicht gut...
 - auch mit Download-Firmware
 - (das war vor ca. drei Jahren...)
- Sticks mit Ralink RT5370 Chipsatz
 - zwar mit non-free Firmware
 - funktioniert aber super!

Hardware: welcher Stick genau?

- https://en.wikipedia.org/wiki/Comparison_of_open-source_wireless_drivers
- Muß „Master (AP) Mode“ unterstützen
- Edimax EW-7612UAn
 - RTL8192cu
 - nicht gut...
 - auch mit Download-Firmware
 - (das war vor ca. drei Jahren...)
- Sticks mit Ralink RT5370 Chipsatz
 - zwar mit non-free Firmware
 - funktioniert aber super!

Hardware: welcher Stick genau?

- https://en.wikipedia.org/wiki/Comparison_of_open-source_wireless_drivers
- Muß „Master (AP) Mode“ unterstützen
- Edimax EW-7612UAn
 - RTL8192cu
 - nicht gut...
 - auch mit Download-Firmware
 - (das war vor ca. drei Jahren...)
- Sticks mit Ralink RT5370 Chipsatz
 - zwar mit non-free Firmware
 - funktioniert aber super!

Hardware: welcher Stick genau?

- https://en.wikipedia.org/wiki/Comparison_of_open-source_wireless_drivers
- Muß „Master (AP) Mode“ unterstützen
- Edimax EW-7612UAn
 - RTL8192cu
 - nicht gut...
 - auch mit Download-Firmware
 - (das war vor ca. drei Jahren...)
- Sticks mit Ralink RT5370 Chipsatz
 - zwar mit non-free Firmware
 - funktioniert aber super!

Hardware: welcher Stick genau?

- https://en.wikipedia.org/wiki/Comparison_of_open-source_wireless_drivers
- Muß „Master (AP) Mode“ unterstützen
- Edimax EW-7612UAn
 - RTL8192cu
 - nicht gut...
 - auch mit Download-Firmware
 - (das war vor ca. drei Jahren...)
- Sticks mit Ralink RT5370 Chipsatz
 - zwar mit non-free Firmware
 - funktioniert aber super!

```
interface=wlan0
driver=nl80211
ssid=xxxxxxxx
country_code=AT
ieee80211d=1
hw_mode=g
channel=1
ieee80211n=1
wpa=2
wpa_passphrase=xxxxxxxx
wps_state=0
```

```
auto wlan0
allow-hotplug wlan0
iface wlan0 inet static
    address 192.168.10.1
    netmask 255.255.255.0
    network 192.168.10.0
    broadcast 192.168.10.255
```

```
# wlan0
subnet 192.168.10.0 netmask 255.255.255.0 {
    range 192.168.10.128 192.168.10.254;
    option routers 192.168.10.1;
    option broadcast-address 192.168.10.255;
}
```

DNS Sperren

- In erster Linie für (bzw. gegen) „Smart“ Devices
- Ohne das Gerät selbst zu „modifizieren“
- Ziel: Zugriff auf „Privacy-feindliche“ Server sperren:
 - Werbung (Browser bzw. In-App)
 - Tracking
 - Facebook
 - ...

- In erster Linie für (bzw. gegen) „Smart“ Devices
- Ohne das Gerät selbst zu „modifizieren“
- Ziel: Zugriff auf „Privacy-feindliche“ Server sperren:
 - Werbung (Browser bzw. In-App)
 - Tracking
 - Facebook
 - ...

- In erster Linie für (bzw. gegen) „Smart“ Devices
- Ohne das Gerät selbst zu „modifizieren“
- Ziel: Zugriff auf „Privacy-feindliche“ Server sperren:
 - Werbung (Browser bzw. In-App)
 - Tracking
 - Facebook
 - ...

- In erster Linie für (bzw. gegen) „Smart“ Devices
- Ohne das Gerät selbst zu „modifizieren“
- Ziel: Zugriff auf „Privacy-feindliche“ Server sperren:
 - Werbung (Browser bzw. In-App)
 - Tracking
 - Facebook
 - ...

- In erster Linie für (bzw. gegen) „Smart“ Devices
- Ohne das Gerät selbst zu „modifizieren“
- Ziel: Zugriff auf „Privacy-feindliche“ Server sperren:
 - Werbung (Browser bzw. In-App)
 - Tracking
 - Facebook
 - ...

- In erster Linie für (bzw. gegen) „Smart“ Devices
- Ohne das Gerät selbst zu „modifizieren“
- Ziel: Zugriff auf „Privacy-feindliche“ Server sperren:
 - Werbung (Browser bzw. In-App)
 - Tracking
 - Facebook
 - ...

- In erster Linie für (bzw. gegen) „Smart“ Devices
- Ohne das Gerät selbst zu „modifizieren“
- Ziel: Zugriff auf „Privacy-feindliche“ Server sperren:
 - Werbung (Browser bzw. In-App)
 - Tracking
 - Facebook
 - ...

Wie funktioniert es?

- Wir haben unseren eigenen DHCP Server
- Erweiterung der Konfiguration, damit Geräte einen eigenen DNS Server verwenden
- DNS Server Installation (dnsmasq)
- Konfiguration um gezielt DNS Namen z.B. auf 127.0.0.1 umzuleiten

Wie funktioniert es?

- Wir haben unseren eigenen DHCP Server
- Erweiterung der Konfiguration, damit Geräte einen eigenen DNS Server verwenden
- DNS Server Installation (dnsmasq)
- Konfiguration um gezielt DNS Namen z.B. auf 127.0.0.1 umzuleiten

Wie funktioniert es?

- Wir haben unseren eigenen DHCP Server
- Erweiterung der Konfiguration, damit Geräte einen eigenen DNS Server verwenden
- DNS Server Installation (dnsmasq)
- Konfiguration um gezielt DNS Namen z.B. auf 127.0.0.1 umzuleiten

Wie funktioniert es?

- Wir haben unseren eigenen DHCP Server
- Erweiterung der Konfiguration, damit Geräte einen eigenen DNS Server verwenden
- DNS Server Installation (dnsmasq)
- Konfiguration um gezielt DNS Namen z.B. auf 127.0.0.1 umzuleiten

```
# wlan0
subnet 192.168.10.0 netmask 255.255.255.0 {
    ...

    option domain-name-servers 192.168.10.1;
}
```

```
interface=eth2  
interface=eth3  
interface=wlan0
```

```
bind-interfaces
```

```
address=/doubleclick.com/127.0.0.1  
address=/facebook.com/127.0.0.1  
address=/googleadservices.com/127.0.0.1  
address=/google-analytics.com/127.0.0.1  
...
```

- Das gibt es alles schon fertig aufbereitet
- <https://pi-hole.net/>
- <https://www.kuketz-blog.de/pi-hole-schwarzes-loch-fuer-werbung-raspberry-pi-teil1>
- Vortrag heute: <https://glt18-programm.linuxtage.at/events/366.html>

- Das gibt es alles schon fertig aufbereitet
- <https://pi-hole.net/>
- <https://www.kuketz-blog.de/pi-hole-schwarzes-loch-fuer-werbung-raspberry-pi-teil1>
- Vortrag heute: <https://glt18-programm.linuxtage.at/events/366.html>

- Das gibt es alles schon fertig aufbereitet
- `https://pi-hole.net/`
- `https://www.kuketz-blog.de/pi-hole-schwarzes-loch-fuer-werbung-raspberry-pi-teil1`
- Vortrag heute: `https://glt18-programm.linuxtage.at/events/366.html`

- Das gibt es alles schon fertig aufbereitet
- <https://pi-hole.net/>
- <https://www.kuketz-blog.de/pi-hole-schwarzes-loch-fuer-werbung-raspberry-pi-teil1>
- Vortrag heute: <https://glt18-programm.linuxtage.at/events/366.html>

Media Streaming

- Filme am Tablet / Handy anschauen
 - ohne daß der Film am Handy gespeichert ist
- Audio auf Verstärker / Handy hören
 - auch über Netzwerk
 - fernsteuerbar
 - <https://humanoids.be/log/2013/01/dlnaaisplay-receiver-bestehend-aus-einem-android-handy/>

- Filme am Tablet / Handy anschauen
 - ohne daß der Film am Handy gespeichert ist
- Audio auf Verstärker / Handy hören
 - auch über Netzwerk
 - fernsteuerbar
 - <https://humanoids.be/log/2013/01/dlnaairplay-receiver-bestehend-aus-einem-android-handy/>

- Filme am Tablet / Handy anschauen
 - ohne daß der Film am Handy gespeichert ist
- Audio auf Verstärker / Handy hören
 - auch über Netzwerk
 - fernsteuerbar
 - <https://humanoids.be/log/2013/01/dlnaairplay-receiver-bestehend-aus-einem-android-handy/>

- Filme am Tablet / Handy anschauen
 - ohne daß der Film am Handy gespeichert ist
- Audio auf Verstärker / Handy hören
 - auch über Netzwerk
 - fernsteuerbar
 - <https://humanoids.be/log/2013/01/dlnaairplay-receiver-bestehend-aus-einem-android-handy/>

- Filme am Tablet / Handy anschauen
 - ohne daß der Film am Handy gespeichert ist
- Audio auf Verstärker / Handy hören
 - auch über Netzwerk
 - fernsteuerbar
 - <https://humanoids.be/log/2013/01/dlnaairplay-receiver-bestehend-aus-einem-android-handy/>

- Filme am Tablet / Handy anschauen
 - ohne daß der Film am Handy gespeichert ist
- Audio auf Verstärker / Handy hören
 - auch über Netzwerk
 - fernsteuerbar
 - <https://humanoids.be/log/2013/01/dlnaairplay-receiver-bestehend-aus-einem-android-handy/>

- DMS: Medienserver
- DMR: Renderer
- DMC: Controller
- DMP: Player (DMC + lokaler DMR)

- DMS: Medienserver
- DMR: Renderer
- DMC: Controller
- DMP: Player (DMC + lokaler DMR)

- DMS: Medienserver
- DMR: Renderer
- DMC: Controller
- DMP: Player (DMC + lokaler DMR)

- DMS: Medienserver
- DMR: Renderer
- DMC: Controller
- DMP: Player (DMC + lokaler DMR)

- DMS: Medienserver
- DMR: Renderer
- DMC: Controller
- DMP: Player (DMC + lokaler DMR)

- Klein und leichtgewichtig
- Ideal für schwache Hardware
- Kann kein Transcoding (Audio und Video)

- Klein und leichtgewichtig
- Ideal für schwache Hardware
- Kann kein Transcoding (Audio und Video)

- Klein und leichtgewichtig
- Ideal für schwache Hardware
- Kann kein Transcoding (Audio und Video)

```
media_dir=A,/var/lib/minidlna/music  
media_dir=V,/var/lib/minidlna/videos  
media_dir=P,/var/lib/minidlna/pictures
```

```
network_interface=eth1  
network_interface=eth2  
network_interface=eth3  
network_interface=wlan0
```

DLNA: Android Apps

App	Server	Renderer	Controller	Player
AirPin(LITE)		x		
AirReceiverLite		x		
ArkMC Lite	x	x	x	?
BubbleUPnp	x	x	x	
DLNA Player				x
DroidUPNP			x	x
MediaHouse			x	
Pixel DMR		x		
UPnPlay		x		

- Habe die genannten durchprobiert
- Verschiedenste Stabilitäts- und Kompatibilitätsprobleme
- Letztendlich: BubbleUPnp + Lizenz
- (eine für alle Android Geräte)

- Habe die genannten durchprobiert
- Verschiedenste Stabilitäts- und Kompatibilitätsprobleme
- Letztendlich: BubbleUPnp + Lizenz
- (eine für alle Android Geräte)

- Habe die genannten durchprobiert
- Verschiedenste Stabilitäts- und Kompatibilitätsprobleme
- Letztendlich: BubbleUPnp + Lizenz
- (eine für alle Android Geräte)

- Habe die genannten durchprobiert
- Verschiedenste Stabilitäts- und Kompatibilitätsprobleme
- Letztendlich: BubbleUPnp + Lizenz
- (eine für alle Android Geräte)

- Android - minidlna: ok
- Verstärker - minidlna: ok
- Aber:
 - Verstärker nicht sichtbar für Android
 - DMS auf Android nicht sichtbar für Verstärker

- Android - minidlna: ok
- Verstärker - minidlna: ok
- Aber:
 - Verstärker nicht sichtbar für Android
 - DMS auf Android nicht sichtbar für Verstärker

- Android - minidlna: ok
- Verstärker - minidlna: ok
- Aber:
 - Verstärker nicht sichtbar für Android
 - DMS auf Android nicht sichtbar für Verstärker

- Android - minidlna: ok
- Verstärker - minidlna: ok
- Aber:
 - Verstärker nicht sichtbar für Android
 - DMS auf Android nicht sichtbar für Verstärker

- Android - minidlna: ok
- Verstärker - minidlna: ok
- Aber:
 - Verstärker nicht sichtbar für Android
 - DMS auf Android nicht sichtbar für Verstärker

- DLNA Geräte „multicasten“ ihre Verfügbarkeit ins Netzwerk
- SSDP funktioniert aber nur im gleichen Subnetz
- Es sei denn...

- DLNA Geräte „multicasten“ ihre Verfügbarkeit ins Netzwerk
- SSDP funktioniert aber nur im gleichen Subnetz
- Es sei denn...

- DLNA Geräte „multicasten“ ihre Verfügbarkeit ins Netzwerk
- SSDP funktioniert aber nur im gleichen Subnetz
- Es sei denn. . .

- static multicast router daemon
- Ermöglicht „Routing“ von Multicast-Paketen
- von je einer Quelle zu einem oder mehreren Zielinterfaces

- static multicast router daemon
- Ermöglicht „Routing“ von Multicast-Paketen
- von je einer Quelle zu einem oder mehreren Zielinterfaces

- static multicast router daemon
- Ermöglicht „Routing“ von Multicast-Paketen
- von je einer Quelle zu einem oder mehreren Zielinterfaces

```
smcroute -a eth3 192.168.3.12 239.255.255.250 wlan0
smcroute -a wlan0 192.168.10.5 239.255.255.250 eth3
smcroute -a wlan0 192.168.10.6 239.255.255.250 eth3
smcroute -a wlan0 192.168.10.8 239.255.255.250 eth3
```

```
iptables -t mangle -A PREROUTING -i eth3 \  
-d 239.255.255.250 -j TTL --ttl-inc 1
iptables -t mangle -A PREROUTING -i wlan0 \  
-d 239.255.255.250 -j TTL --ttl-inc 1
```

Q & A