

DualStack IPv6 mit 1&1 auf dem EdgeRouter PoE 5-Port

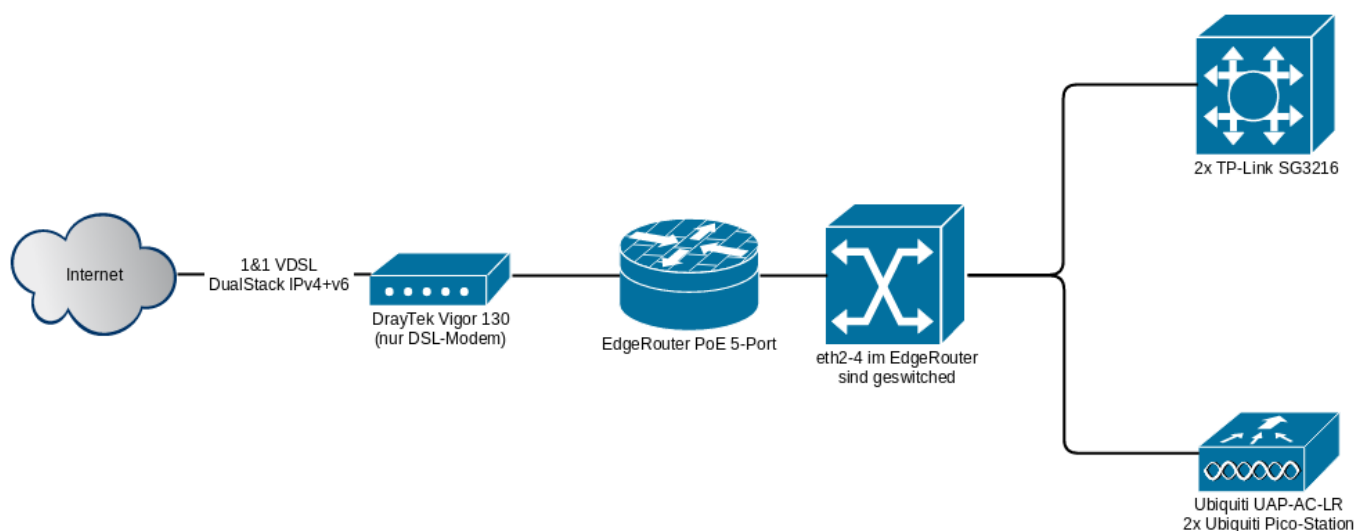
Zuletzt getestet am 08.07.2016

Schon seit einiger Zeit kann man mit Telekom, bzw. den Reseller-Anschlüssen von 1&1 DualStack [IPv6](#) fahren (laut verschiedenen Quellen aber nur bei VDSL). In diesem Artikel will ich meine Konfiguration vorstellen.

meine aktuelle Hardware

- DSL-Modem DrayTek Vigor 130 (wie man das mit 1&1 VDSL50 einrichtet kann man [hier](#) nachlesen)
- Ubiquiti EdgeRouter PoE 5-Port
- 2x TP-Link TL-SG3216 Managed Switches
- Ubiquiti UAP-AC-LR
- 2x Ubiquiti Pico-Station M2
- TP-Link WR1043ND (für Freifunk)

mein aktuelles Netzwerksetup



VLANS

- Management VLAN untagged
- VLAN 10 - mein eigenes Netz
- VLAN 11 - eingeschränktes Gästernetzwerk
- VLAN 20 - Freifunk Client-Netz
- VLAN 21 - Freifunk BATMAN
- VLAN 22 - Freifunk WAN (Uplink für einen Router, hätte ich auch ins Gästernetz stecken können)

IPv6 benötige ich für die VLANs 10 und 11. In den Übrigen ist es aktuell nicht notwendig oder nicht erwünscht.

Ports am EdgeRouter

- eth0 - geht zum LAN-Port des DrayTek DSL-Modems
- eth1 - unbelegt
- eth2-4 - Zusammengefasst zu switch0
- switch0
 - Uplink mit PoE zum WLAN AP (Ubiquiti UAP-AC-LR)
 - Uplink zu den beiden TP-Link Managed Switchen

Konfiguration des Routers

Ich zeige hier nur die relevanten Teile als „show configuration commands“ (also zum einfachen Übernehmen per Copy&Paste). Meine komplette Konfiguration (ohne Passwörter und private Teile natürlich) kann man sich hier anschauen.

Vor dem EdgeRouter hängt ein DrayTek Vigor 130 (als reines DSL-Modem konfiguriert). Die PPPoE Einwahl konfiguriere ich also im EdgeRouter.

Zuerst die IPv6 Firewall für das WAN-Interface pppoe0:

```
set firewall ipv6-name WAN_IN_v6 default-action drop
set firewall ipv6-name WAN_IN_v6 description 'incoming IPv6 traffic to local networks'
set firewall ipv6-name WAN_IN_v6 enable-default-log
set firewall ipv6-name WAN_IN_v6 rule 1 action accept
set firewall ipv6-name WAN_IN_v6 rule 1 description 'Allow established/related'
set firewall ipv6-name WAN_IN_v6 rule 1 log disable
set firewall ipv6-name WAN_IN_v6 rule 1 protocol all
set firewall ipv6-name WAN_IN_v6 rule 1 state established enable
set firewall ipv6-name WAN_IN_v6 rule 1 state invalid disable
set firewall ipv6-name WAN_IN_v6 rule 1 state new disable
set firewall ipv6-name WAN_IN_v6 rule 1 state related enable
set firewall ipv6-name WAN_IN_v6 rule 2 action drop
set firewall ipv6-name WAN_IN_v6 rule 2 description 'Drop invalid state'
set firewall ipv6-name WAN_IN_v6 rule 2 log disable
set firewall ipv6-name WAN_IN_v6 rule 2 protocol all
set firewall ipv6-name WAN_IN_v6 rule 2 state established disable
set firewall ipv6-name WAN_IN_v6 rule 2 state invalid enable
set firewall ipv6-name WAN_IN_v6 rule 2 state new disable
set firewall ipv6-name WAN_IN_v6 rule 2 state related disable
set firewall ipv6-name WAN_IN_v6 rule 3 action accept
set firewall ipv6-name WAN_IN_v6 rule 3 description 'allow icmpv6'
set firewall ipv6-name WAN_IN_v6 rule 3 log disable
set firewall ipv6-name WAN_IN_v6 rule 3 protocol icmpv6
set firewall ipv6-name WAN_LOCAL_v6 default-action drop
set firewall ipv6-name WAN_LOCAL_v6 description 'incoming IPv6 traffic to EdgeRouter'
set firewall ipv6-name WAN_LOCAL_v6 enable-default-log
set firewall ipv6-name WAN_LOCAL_v6 rule 1 action accept
set firewall ipv6-name WAN_LOCAL_v6 rule 1 description 'Allow established/related'
set firewall ipv6-name WAN_LOCAL_v6 rule 1 log disable
set firewall ipv6-name WAN_LOCAL_v6 rule 1 protocol all
set firewall ipv6-name WAN_LOCAL_v6 rule 1 state established enable
set firewall ipv6-name WAN_LOCAL_v6 rule 1 state invalid disable
set firewall ipv6-name WAN_LOCAL_v6 rule 1 state new disable
set firewall ipv6-name WAN_LOCAL_v6 rule 1 state related enable
set firewall ipv6-name WAN_LOCAL_v6 rule 2 action drop
set firewall ipv6-name WAN_LOCAL_v6 rule 2 description 'Drop invalid state'
set firewall ipv6-name WAN_LOCAL_v6 rule 2 log disable
set firewall ipv6-name WAN_LOCAL_v6 rule 2 protocol all
set firewall ipv6-name WAN_LOCAL_v6 rule 2 state established disable
set firewall ipv6-name WAN_LOCAL_v6 rule 2 state invalid enable
set firewall ipv6-name WAN_LOCAL_v6 rule 2 state new disable
set firewall ipv6-name WAN_LOCAL_v6 rule 2 state related disable
set firewall ipv6-name WAN_LOCAL_v6 rule 3 action accept
set firewall ipv6-name WAN_LOCAL_v6 rule 3 description 'allow icmpv6'
set firewall ipv6-name WAN_LOCAL_v6 rule 3 log disable
set firewall ipv6-name WAN_LOCAL_v6 rule 3 protocol icmpv6
set firewall ipv6-name WAN_LOCAL_v6 rule 4 action accept
set firewall ipv6-name WAN_LOCAL_v6 rule 4 description 'allow dhcpv6'
set firewall ipv6-name WAN_LOCAL_v6 rule 4 destination port 546
```

```

set firewall ipv6-name WAN_LOCAL_v6 rule 4 protocol udp
set firewall ipv6-name WAN_LOCAL_v6 rule 4 source port 547
set firewall ipv6-name WAN_OUT_v6 default-action accept
set firewall ipv6-name WAN_OUT_v6 description 'outgoing IPv6 traffic'
set firewall ipv6-receive-redirects disable
set firewall ipv6-src-route disable
set firewall options mss-clamp interface-type all
set firewall options mss-clamp mss 1452
set firewall options mss-clamp6 interface-type all
set firewall options mss-clamp6 mss 1412
set firewall receive-redirects disable
set firewall send-redirects enable
set firewall source-validation disable
set firewall syn-cookies enable
set firewall ip-src-route disable
set firewall log-martians enable

```

Damit werden DHCPv6 und ICMPv6 eingehend auf den Router erlaubt. established und related Pakete dürfen auch in die internen Netze und ausgehend ist über v6 alles erlaubt.

Der PPPoE-Teil sieht so aus:

```

set interfaces ethernet eth0 address 192.168.xxx.2/24
set interfaces ethernet eth0 description 'Internet (PPPoE)'
set interfaces ethernet eth0 duplex auto
set interfaces ethernet eth0 speed auto
set interfaces ethernet eth0 pppoe 0 default-route auto
set interfaces ethernet eth0 pppoe 0 description 'l&l VDSL-50'
set interfaces ethernet eth0 pppoe 0 dhcpv6-pd pd 0 interface switch0 host-address '::1dle:f001'
set interfaces ethernet eth0 pppoe 0 dhcpv6-pd pd 0 interface switch0 no-dns
set interfaces ethernet eth0 pppoe 0 dhcpv6-pd pd 0 interface switch0 prefix-id 0
set interfaces ethernet eth0 pppoe 0 dhcpv6-pd pd 0 interface switch0 service slaac
set interfaces ethernet eth0 pppoe 0 dhcpv6-pd pd 0 interface switch0.10 host-address ':::dead:be
set interfaces ethernet eth0 pppoe 0 dhcpv6-pd pd 0 interface switch0.10 no-dns
set interfaces ethernet eth0 pppoe 0 dhcpv6-pd pd 0 interface switch0.10 prefix-id 10
set interfaces ethernet eth0 pppoe 0 dhcpv6-pd pd 0 interface switch0.10 service slaac
set interfaces ethernet eth0 pppoe 0 dhcpv6-pd pd 0 interface switch0.11 host-address ':::b00b:ba
set interfaces ethernet eth0 pppoe 0 dhcpv6-pd pd 0 interface switch0.11 no-dns
set interfaces ethernet eth0 pppoe 0 dhcpv6-pd pd 0 interface switch0.11 prefix-id 11
set interfaces ethernet eth0 pppoe 0 dhcpv6-pd pd 0 interface switch0.11 service slaac
set interfaces ethernet eth0 pppoe 0 dhcpv6-pd pd 0 prefix-length 56
set interfaces ethernet eth0 pppoe 0 dhcpv6-pd prefix-only
set interfaces ethernet eth0 pppoe 0 dhcpv6-pd rapid-commit enable
set interfaces ethernet eth0 pppoe 0 firewall in ipv6-name WAN_IN_v6
set interfaces ethernet eth0 pppoe 0 firewall in name WAN_IN
set interfaces ethernet eth0 pppoe 0 firewall local ipv6-name WAN_LOCAL_v6
set interfaces ethernet eth0 pppoe 0 firewall local name WAN_LOCAL
set interfaces ethernet eth0 pppoe 0 firewall out ipv6-name WAN_OUT_v6
set interfaces ethernet eth0 pppoe 0 firewall out name WAN_OUT
set interfaces ethernet eth0 pppoe 0 ipv6 address autoconf
set interfaces ethernet eth0 pppoe 0 ipv6 dup-addr-detect-transmits 1
set interfaces ethernet eth0 pppoe 0 ipv6 enable
set interfaces ethernet eth0 pppoe 0 mtu 1492
set interfaces ethernet eth0 pppoe 0 name-server auto
set interfaces ethernet eth0 pppoe 0 password XXXXXXXXXXXXXXXXXXXX
set interfaces ethernet eth0 pppoe 0 user-id Hlund1/pt1234-567@online.de

```

Weitere Konfiguration ist nicht mehr nötig. Die internen Netze werden per DHCP Prefix-Delegation und SLAAC (Clients erzeugen sich ihre Adresse selbst mit dem entsprechenden Prefix) mit IPv6-Adressen versorgt. Dabei habe ich den Interfaces auf dem Gateway „sprechende IPs“ verpasst ;)

IPv6 Privacy Extensions

Es empfiehlt sich die IPv6 Privacy Extensions zu aktivieren, sofern diese nicht bereits standardmäßig aktiv sind. Wenn diese nicht aktiviert sind, läßt sich der eigene Client ziemlich leicht anhand der in der IPv6 Adresse vorhandenen MAC-Adresse verfolgen bzw. wieder erkennen. Wie sich die Privacy Extensions aktivieren lassen, kann man z.B. in diesem [Artikel auf heise.de](#) nachlesen.

