

IPv6 mit OpenWRT (Einführung)

Tutorial

Dr. Peter Bieringer
Deep Space 6
peter@deepspace6.net
<http://www.deepspace6.net/>



IPv6-Kongress
Frankfurt/Main, Deutschland
10. - 11. Mai 2012
<http://www.ipv6-kongress.de/>

Inhalt

IPv6 mit OpenWRT (Einführung)

- ▶ **Allgemeines**
- ▶ **Voraussetzungen & Empfehlungen**
- ▶ **IPv6-Konfiguration**
- ▶ **IPv6-Anbindungen**
 - ◆ PPPv6 & DHCPv6
 - ◆ SixXS
 - ◆ gogo6
- ▶ **Absicherung & Firewalling**
- ▶ **Fehlersuche**

Allgemeines zu OpenWRT

Allgemeines zu OpenWRT

- ◆ **OpenWRT basiert auf Linux**
- ◆ **Schnittstellen**
 - ◆ Interne Schnittstellen üblicherweise als Linux-Bridges definiert
 - ◆ Z.B: br-lan, br-guest
 - ◆ Externe Schnittstelle (“Uplink”) u.a.
 - ◆ PPPoE
 - ◆ DHCPv4
 - ◆ Statisch
- ◆ **Administration**
 - ◆ Web-Oberfläche
 - ◆ Via SSH und Konfigurationsdateien

Voraussetzungen für IPv6 in OpenWRT

IPv6 in OpenWRT

Voraussetzungen - Version

◆ Welche Version?

- ◆ IPv6-Unterstützung seit *Kamikaze Version 7*
- ◆ Empfohlen: *Backfire Version 10.03.1*
 - ◆ Aktuelle Version!
 - ◆ IPv6-Unterstützung der Firewall brauchbar!

IPv6 in OpenWRT

Voraussetzungen - Basis

▶ IPv6-Kernelmodul installiert?

◆ Test

```
# opkg list_installed | grep kmod-ipv6  
kmod-ipv6 - 2.6.32.27-1
```

◆ Installation

```
# opkg update  
# opkg install kmod-ipv6
```

▶ IPv6 Kernelmodul aktiv?

◆ Test

```
# wc -l /proc/net/if_inet6  
29 /proc/net/if_inet6
```

IPv6 in OpenWRT

Voraussetzungen - Erweiterung

- ▶ **Router Advertisement -Programm “radvd”**

- ◆ Installation

- ```
opkg install radvd
```

- ▶ **IPv6-Firewall-Erweiterung installiert?**

- ◆ Installation

- ```
# opkg install kmod-ip6tables ip6tables
```


Empfehlungen (nicht nur) für IPv6 in OpenWRT

IPv6 in OpenWRT

Empfehlungen

◆ Remote-Syslog aktivieren

- ◆ Sehr hilfreich für Debugging on-the-fly

- ◆ Syslog-Konfiguration

 - ◆ Datei: /etc/config/system

```
config 'system'  
    option 'log_ip' '192.168.1.2'
```

- ◆ Syslog-Ziel:

 - ◆ Konfiguration für z.B. rsyslog:

 - ◆ Datei: /etc/rsyslog.d/openwrt.conf

```
:fromhost-ip, isequal, "192.168.1.1" /var/log/openwrt  
& ~
```

 - ◆ Ggf. logrotate-Konfiguration erweitern

 - ◆ Beispielkonfiguration: siehe Notizen

IPv6-Konfiguration von OpenWRT

IPv6-Konfiguration

◆ Statisch

- ◆ IPv6-Adresse
- ◆ Routing
- ◆ Router-Advertisements

IPv6-Adresskonfiguration

Ansicht

◆ Werkzeuge `ifconfig`

◆ oder `ip` (muß erst installiert werden)

```
# ifconfig INTERFACE
```

```
# ip -6 addr show dev INTERFACE
```

◆ Beispiele

```
# ifconfig br-lan
```

```
br-lan    Link encap:Ethernet  HWaddr 00:12:17:01:23:45
          inet addr:192.168.17.1  Bcast:192.168.17.255  Mask:255.255.255.0
          inet6 addr: 2001:6f8:133d:1::1/64  Scope:Global
          inet6 addr: fe80::212:17ff:fe01:2345/64  Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:360447  errors:0  dropped:0  overruns:0  frame:0
          TX packets:254666  errors:0  dropped:0  overruns:0  carrier:0
          collisions:0  txqueuelen:0
          RX bytes:58867265 (56.1 MiB)  TX bytes:230469793 (219.7 MiB)
```

IPv6-Adresskonfiguration

Statische Zuweisung (1)

- ◆ Konfigurationsdatei: `/etc/config/network`

```
config 'interface' 'lan'  
    option 'type' 'bridge'  
    option 'ifname' 'eth0.0'  
    option 'proto' 'static'  
    option 'netmask' '255.255.255.0'  
    option 'ipaddr' '192.168.17.1'  
    option 'ip6addr' '2001:6f8:133d:1::1/64'
```

IPv6-Adresskonfiguration

Statische Zuweisung (2)

gate6pbg | OpenWrt Backfire 10.03.1 | Load: 0.28 0.06 0.02 | Auto Refresh: **on** Changes: 0

Status System Services **Network** Logout

Interfaces Wifi Switch DHCP and DNS Hostnames Static Routes Diagnostics Firewall Radvd

WAN GUEST WAN6 **LAN**

Interfaces - LAN

On this page you can configure the network interfaces. You can bridge several interfaces by ticking the "bridge interfaces" field and enter the names of several network interfaces separated by spaces. You can also use VLAN notation INTERFACE.VLANNR (e.g.: eth0.1).

Common Configuration

General Setup **Advanced Settings** Physical Settings Firewall Settings

Status **Uptime:** 22d 17h 17m 13s
MAC Address: 00:12:17:07:B9:DC
RX: 59.09 MB (362124 Pkts.)
TX: 230.70 MB (255688 Pkts.)
IPv4: 192.168.17.1/24
IPv6: 2001:6f8:133d:1:0:0:0:1/64, FE80:0:0:0:212:17FF:FE [REDACTED]/64

Protocol **Static address**

IPv4 address **192.168.17.1**

IPv4 netmask **255.255.255.0**

IPv4 gateway

IPv4 broadcast

Use custom DNS servers

Accept router advertisements

Send router solicitations

IPv6 address **2001:6f8:133d:1::1/64**

IPv6 gateway

IPv6-Routing Ansicht

◆ Werkzeuge route

- ◆ oder `ip` (muß erst installiert werden)

```
# route -n -A inet6
```

```
# ip -6 route show [dev INTERFACE]
```

◆ Beispiele

```
# route -n -A inet6 | grep br-lan
```

<code>2001:6f8:133d:1::/64</code>	<code>::</code>	<code>U</code>	<code>256</code>	<code>0</code>	<code>0</code>	<code>br-lan</code>
<code>fe80::/64</code>	<code>::</code>	<code>U</code>	<code>256</code>	<code>0</code>	<code>0</code>	<code>br-lan</code>
<code>ff00::/8</code>	<code>::</code>	<code>U</code>	<code>256</code>	<code>0</code>	<code>0</code>	<code>br-lan</code>

IPv6-Routing Konfiguration (1)

◆ Konfigurationsdatei: /etc/config/network

```
config 'route6'  
    option 'interface' 'lan'  
    option 'target' 'fec0:0:0:2::/64'  
    option 'gateway' 'fec0:0:0:1::2/64'
```

IPv6-Routing Konfiguration (2)

gate6pbg | OpenWrt Backfire 10.03.1 | Load: 0.15 0.04 0.05 Changes: 0

Status System Services **Network** Logout

Interfaces Wifi Switch DHCP and DNS Hostnames **Static Routes** Diagnostics Firewall Radvd

Routes

Routes specify over which interface and gateway a certain host or network can be reached.

Static IPv4 Routes

Interface	Target <small>Host-IP or Network</small>	IPv4-Netmask <small>if target is a network</small>	IPv4-Gateway	Metric	MTU
<i>This section contains no values yet</i>					

Static IPv6 Routes

Interface	Target <small>IPv6-Address or Network (CIDR)</small>	IPv6-Gateway	Metric	MTU
lan	fec0:0:0:2::/64	fec0:0:0:1::2/64	0	1500

IPv6-Adresskonfiguration

Router Advertisements (1)

◆ Konfigurationsdatei: /etc/config/radvd

```
config 'interface'
```

```
option 'interface' 'lan'  
option 'AdvSendAdvert' '0'  
option 'IgnoreIfMissing' '1'  
option 'AdvSourceLLAddress' '1'  
option 'AdvDefaultPreference' 'medium'  
option 'MinRtrAdvInterval' '30'  
option 'MaxRtrAdvInterval' '120'
```

```
config 'prefix'
```

```
option 'ignore' '0'  
option 'interface' 'lan'  
option 'AdvOnLink' '1'  
option 'AdvAutonomous' '1'  
list 'prefix' '2001:6f8:133d:0001::/64'
```

IPv6-Adresskonfiguration

Router Advertisements (2)

gate6pbg | OpenWrt Backfire 10.03.1 | Load: 0.37 0.35 0.15 Changes: 0

Status System Services **Network** Logout

Interfaces Wifi Switch DHCP and DNS Hostnames Static Routes Diagnostics Firewall **Radvd**

Radvd

Radvd is a router advertisement daemon for IPv6. It listens to router solicitations and sends router advertisements as described in RFC 4861.

Interfaces

Enable	Interface	Multicast	Advertising	Max. interval	Mobile IPv6	Preference	
<input checked="" type="checkbox"/>	lan:	<input checked="" type="checkbox"/>	no	120s	no	medium	

Prefixes

Enable	Interface	Prefix	Autonomous On-link Validity time				
<input checked="" type="checkbox"/>	lan:	<input checked="" type="checkbox"/> 2001:6F8:133D:1:0:0:0:1/64	<input checked="" type="checkbox"/>	yes	yes	86400	

Routes

Enable	Interface	Prefix	Lifetime	Preference	
<input type="checkbox"/>	lan:	2001:6F8:133D:1:0:0:0:1/64	1800	medium	

RDNSS

Enable	Interface	Address	Lifetime	
<input type="checkbox"/>	lan:	2001:6F8:133D:1:0:0:0:1/64	1200	

DNSSL

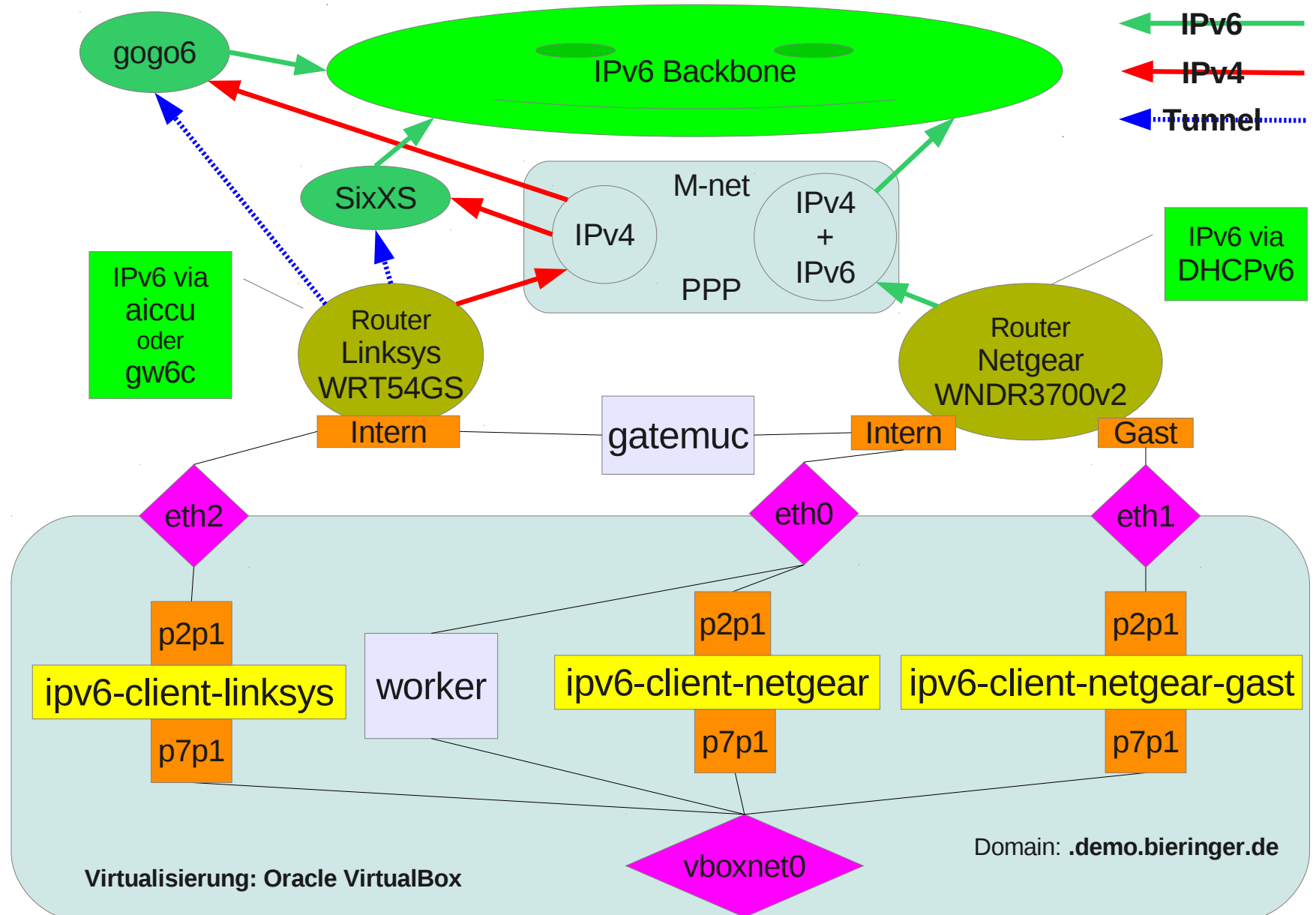
Enable	Interface	Suffix	Lifetime	
<input type="checkbox"/>	lan:	?	1200	

IPv6-Anbindungen

IPv6-Anbindungen

- ◆ **PPPo6 & DHCPv6**
- ◆ **Tunnel via SixXS**
- ◆ **Tunnel via gogo6**

Aufbau Demonstration

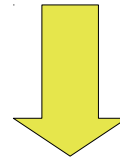


Zugang via PPPv6 & DHCPv6

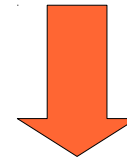
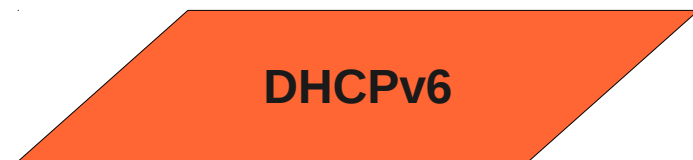
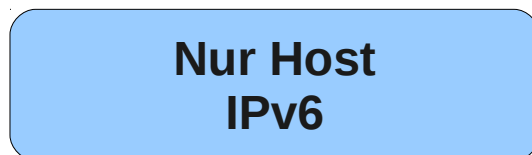
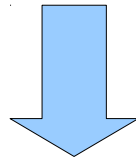
PPP für IPv6

- ◆ **PPPo6 ist definiert in RFC 5072 (ex 2472)**

- ◆ NUR Aushandlung beidseitiger link-local-Adressen
- ◆ KEINE explizite Präfix- bzw. globale Adress-Aushandlung



- ◆ Ohne Zusatzprotokolle keine globale IPv6-Kommunikation



DHCP für IPv6

◆ DHCPv6 definiert in RFC 3315

- ◆ Arbeitet mit link-local-Adressen
- ◆ Wichtige Option: DHCPv6 Präfix-Delegation (RFC 3633)
- ◆ DHCP-Server
 - ◆ Port: udp/547
- ◆ Client
 - ◆ Adresse: link-local
 - ◆ Port: udp/546 (source-port bind)
 - ◆ Ziel: ff02::1:2 (Multicast: alle DHCP-Agenten am Link)



- ◆ Probleme mit Stateful Firewall durch zusätzliche Regeln lösen
 - ◆ Client & Client: stateless

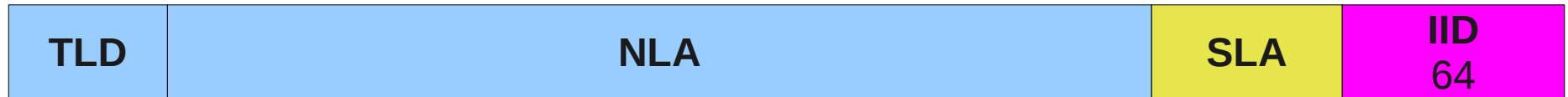
PPP / DHCP für IPv6

◆ “Connect”

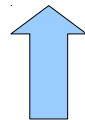
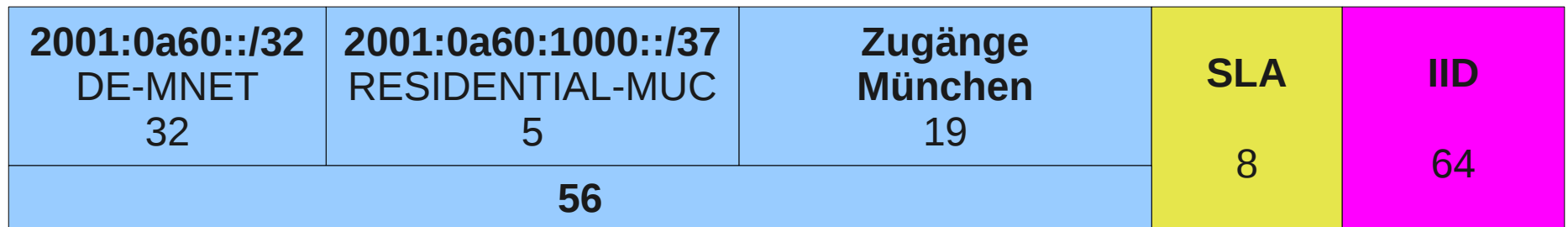
- ◆ Startet PPP (oder PPPoE)
 - ◆ PPPv6: Handelt link-local Adresse aus
- ◆ Startet DHCPv6 Client
 - ◆ Client sendet DHCPv6-Anfrage incl. Präfix-Anfrage
 - ◆ Server sendet DHCPv6-Antwort samt Präfix
 - ◆ Client konfiguriert ein oder mehrere Schnittstellen abhängig von lokal vorher definierten SLA
- ◆ Client (re-)startet Router Advertisement Daemon mit neuen Präfixes

Adresszuweisung via DHCPv6

♦ Generell



♦ M-net (München)



Präfix via
DHCPv6



Lokale
Konfiguration

IPv6 nativ via PPPv6 & DHCPv6



◆ ISP: M-net

- ◆ IPv4: IPv6-Präfix für PPP-Schnittstelle via RA
 - ◆ PPP-Benutzer: `Xxxxxx@mdsl.mnet-online.de'`
- ◆ IPv6-Test: via DHCPv6
 - ◆ PPP-Benutzer: `Xxxxxx@v6.mnet-online.de'`

◆ OpenWRT-Konfiguration

- ◆ IPv6 aktiv für WAN-Schnittstelle
 - ◆ “Enable IPv6 negotiation on the PPP link”
- ◆ DHCPv6 konfiguriert
 - ◆ CLI-Konfiguration notwendig
- ◆ Radvd konfiguriert
 - ◆ Mit generischem Präfix den jeweilig zugewiesenen verteilen
 - ◆ Präfix: `0:0:0:0:0:0:0:0/64`

IPv6 nativ via PPPv6 & DHCPv6

◆ Funktionsweise in OpenWRT

- ◆ Herstellung PPP-Verbindung
- ◆ Starten von dhcp6c via Hotplug
 - ◆ IPv6-Präfix von ISP via DHCPv6
 - ◆ Präfix + konfigurierter SLA pro Schnittstelle => Adresse zuweisen
 - ◆ Restart von Radvd via Hotplug

IPv6 nativ via PPPv6 & DHCPv6 Installation

- ▶ Paket “dhcp6-client” fehlen Hotplug-Skripte
- ▶ Paket “wide-dhcp6c-client” installieren

```
# opkg install wide-dhcpv6-client
```

IPv6 nativ via PPPv6 & DHCPv6 Konfiguration RADVD

- ▶ **Später via DHCPv6 zugewiesener Präfix durch den ISP nicht bekannt**
 - ◆ Spezialkonfiguration für RADVD notwendig
 - ◆ Spezial-Präfix: `::/64` pro Schnittstelle
 - ◆ RADVD konfiguriert bei "reload" pro definierter Schnittstelle automatisch von JEDER existierenden IPv6-Adresse
- ▶ **Konfigurationsdatei: `/etc/config/radvd`**

```
config 'prefix'  
    option 'ignore'          '0'  
    option 'interface'      'lan'  
    option 'AdvOnLink'      '1'  
    option 'AdvAutonomous'  '1'  
    list 'prefix'           '::<64'
```


IPv6 nativ via PPPv6 & DHCPv6

Konfiguration PPPv6 (1)

- ◆ Konfiguration über WebUI oder CLI möglich
- ◆ Datei: /etc/config/network

```
config 'interface' 'wan'  
    option '_orig_ifname' 'eth1'  
    option '_orig_bridge' 'false'  
    option 'proto' 'pppoe'  
    option 'password' 'SECRET'  
    option 'ipv6' '1'  
    option 'ifname' 'eth1'  
    option 'username' 'XA.....@v6.mnet-online.de'
```

IPv6 nativ via PPPv6 & DHCPv6 Konfiguration PPPv6 (2)

gate6muc.muc.bieringer.de | OpenWrt Backfire 10.03.1 | Load: 0.00 0.10 0.10 | Auto Refresh: **on** Changes:

Status System Services **Network** Logout

Interfaces Wifi Switch DHCP and DNS Hostnames Static Routes Diagnostics Firewall Radvd


WAN GUEST LAN

Interfaces - WAN

On this page you can configure the network interfaces. You can bridge several interfaces by ticking the "bridge interfaces" field and enter the names of several network interfaces separated by spaces. You can also use VLAN notation INTERFACE.VLANNR (e.g.: eth0.1).

Common Configuration

General Setup **Advanced Settings** Physical Settings Firewall Settings

Bring up on boot	<input checked="" type="checkbox"/>
Enable IPv6 negotiation on the PPP link	<input checked="" type="checkbox"/> 
Use default gateway	<input checked="" type="checkbox"/> ⓘ If unchecked, no default route is configured
Use gateway metric	<input type="text" value="0"/>
Use DNS servers advertised by peer	<input checked="" type="checkbox"/> ⓘ If unchecked, the advertised DNS server addresses are ignored
LCP echo failure threshold	<input type="text" value="0"/> ⓘ Presume peer to be dead after given amount of LCP echo failures, use 0 to ignore failures
LCP echo interval	<input type="text" value="5"/> ⓘ Send LCP echo requests at the given interval in seconds, only effective in conjunction with failure threshold
Inactivity timeout	<input type="text" value="0"/> ⓘ Close inactive connection after the given amount of seconds, use 0 to persist connection

IPv6 nativ via PPPv6 & DHCPv6

Aktivierung PPPv6

◆ (Re-)Connect der WAN-Schnittstelle (oder Reboot)

```
# kill -SIGHUP `pidof pppd`
```

◆ Logging (Auszug)

```
pppd: Connect: pppoe-wan <--> eth1  
pppd: primary   DNS address 212.18.0.5  
pppd: secondary DNS address 212.18.3.5  
pppd: local    LL address fe80::ac92:0102:d101:2345  
pppd: remote  LL address fe80::0090:1a00:0201:2345
```

IPv6 nativ via PPPv6 & DHCPv6

Test PPPv6

◆ PPP-Schnittstelle nach erfolgter Einwahl

```
# ifconfig pppoe-wan
```

```
pppoe-wan Link encap:Point-to-Point Protocol
```

```
inet addr:93.104.1.1 P-t-P:82.135.1.1 Mask:255.255.255.255
```

```
inet6 addr: fe80::f105:52d3:fe01:2345/10 Scope:Link
```

```
UP POINTOPOINT RUNNING NOARP MULTICAST MTU:1492 Metric:1
```

◆ Test

```
# ping6 -I pppoe-wan -c 1 fe80::0090:1a00:0201:2345
```

```
PING fe80::0090:1a00:0201:2345 (fe80::90:1a00:201:2345): 56 data bytes
```


```
64 bytes from fe80::90:1a00:201:2345: seq=0 ttl=255 time=8.487 ms
```

```
--- fe80::0090:1a00:0201:2345 ping statistics ---
```

```
1 packets transmitted, 1 packets received, 0% packet loss
```

```
round-trip min/avg/max = 8.487/8.487/8.487 ms
```

IPv6 nativ via PPPv6 & DHCPv6 Konfiguration DHCPv6 (1)

- ◆ **Konfiguration nur über CLI aktuell möglich**
 - ◆ Keine Unterstützung via WebUI “luci”
- ◆ **Konfiguration anpassen**
 - ◆ für interne Schnittstelle “br-lan”
 - ◆ für loopback-Schnittstelle “lo”
 - ◆ Router selbst bekommt damit globale IPv6-Adresse
 - ◆ Vereinfacht IPv6-Verbindungstests
 - ◆ Erreichbar von außen 
- ◆ **Logging**
 - ◆ Für erste Tests “debug” aktivieren
 - ◆ Externer Syslog-Server sehr hilfreich dabei

IPv6 nativ via PPPv6 & DHCPv6

Konfiguration DHCPv6 (2)

◆ Datei: /etc/config/dhcp6c

```
config 'dhcp6c' 'basic'
    option 'enabled' '1'
    option 'interface' 'wan' # This is the interface the DHCPv6 client will run on
    option 'pd' '1' # Prefix Delegation
    option 'rapid_commit' '1' # Rapid Commit
    option 'domain_name_servers' '1'
    option 'debug' '1'

config 'interface' 'loopback'
    option 'enabled' '1'
    option 'sla_id' '0'
    option 'sla_len' '8' # (M-net verteilt /56)

config 'interface' 'lan'
    option 'enabled' '1'
    option 'sla_id' '1'
    option 'sla_len' '8' # (M-net verteilt /56)
```

IPv6 nativ via PPPv6 & DHCPv6

Konfiguration DHCPv6 (3)

◆ Erzeugte Konfiguration: /tmp/etc/dhcp6c.conf

```
interface pppoe-wan {
    send ia-pd 0;
    send rapid-commit;
    script "/usr/bin/dhcp6c-state";
    request domain-name-servers;
};

id-assoc pd 0 {
    prefix-interface lo {
        sla-id 0;
        sla-len 8;
    };
    prefix-interface br-lan {
        sla-id 1;
        Sla-len 8;
    };
};
```

IPv6 nativ via PPPv6 & DHCPv6

Aktivierung DHCPv6

◆ (Re-)Start von DHCPv6

- ◆ auch möglich: PPP-Reconnect oder Reboot

```
# /etc/init.d/dhcp6c restart
```

◆ Logging (Auszug)

```
dhcp6c: client6_send: send solicit to ff02::1:2
dhcp6c: client6_recv: receive reply from fe80::90:1a00:201:2345 on pppoe-wan
dhcp6c: update_prefix: create a prefix 2001:a60:1201:0000::/56 pltime=1800, ...
dhcp6c: ifaddrconf: add an address 2001:a60:1201:0000:200:ff:fe00:0/64 on lo
dhcp6c: ifaddrconf: add an address 2001:a60:1201:0001:a221:b7ff:fe01:2345/64 on br-lan
dnsmasq: using nameserver 2001:a60::53:2#53
dnsmasq: using nameserver 2001:a60::53:1#53
dnsmasq: using nameserver 212.18.0.5#53
dnsmasq: using nameserver 212.18.3.5#53
```


IPv6 nativ via PPPv6 & DHCPv6

DUID Problem DHCPv6

- ▶ **DHCPv6 verwendet DUID (DHCP Unique Identifier)**
 - ▶ DHCPv4 verwendet MAC-Adresse
- ▶ **Mögliches Problem: Ableitung der DUID nicht möglich**

```
dhcp6c: starting dhcp6c
```

```
dhcp6c: Unable to derive DUID from interface 'pppoe-wan' and no valid user DUID given
```

```
dhcp6c: get_duid: DUID file corrupted
```

```
dhcp6c: client6_init: failed to get a DUID
```

- ▶ **Manuelle Definition als Lösung**
 - ▶ DUID manuell ableiten von interner **MAC-Adresse** (DUID-LL)
 - ▶ Präfix: **00:03** (DUID-LL) **00:06** (Ethernet)
 - ▶ Datei: /etc/config/dhcp6c

```
config 'dhcp6c' 'basic'
```

```
# The given value must be uppercase and globally unique!
```

```
option 'duid' '00:03:00:06:A0:21:B7:01:23:45'
```

IPv6 nativ via PPPv6 & DHCPv6

Test DHCPv6

◆ Schnittstellen nach erfolgreichem DHCPv6

```
# ifconfig lo
lo          Link encap:Local Loopback
           inet addr:127.0.0.1  Mask:255.0.0.0
           inet6 addr: ::1/128 Scope:Host
           inet6 addr: 2001:a60:1201:0000:200:ff:fe00:0/64 Scope:Global
           UP LOOPBACK RUNNING  MTU:16436  Metric:1

# ifconfig br-lan
br-lan     Link encap:Ethernet  HWaddr A0:21:B7:01:23:45
           inet addr:192.168.1.1  Bcast:192.168.1.255  Mask:255.255.255.0
           inet6 addr: 2001:a60:1201:41cb::1/64 Scope:Global
           inet6 addr: 2001:a60:1201:4101:a221:b7ff:fe01:2345/64 Scope:Global
           inet6 addr: fe80::a221:b7ff:fe01:2345/64 Scope:Link
```

◆ Test

```
# ping6 -c 1 www.ipv6.bieringer.de
PING www.ipv6.bieringer.de (2001:4dd0:f838:a006::6): 56 data bytes
64 bytes from 2001:4dd0:f838:a006::6: seq=0 ttl=52 time=56.198 ms
```



Zugang via SixXS

IPv6 via Tunnel zu ISP SixXS Installation



- ▶ **NTP-Synchronisation notwendig!**
- ▶ **“ip” installieren (Abhängigkeiten)**

```
# opkg install ip
```

- ▶ **Tunnel-Programm “aiccu” installieren**

```
# opkg install aiccu
```

IPv6 via Tunnel zu ISP SixXS Konfiguration

- ◆ Konfigurationsdatei: `/etc/config/aiccu`



```
config aiccu
```

```
option username      'PB530-RIPE/Txxxx'  
option password     'SECRETPASSWORD'  
option protocol     'tic'  
option server       'tic.sixxs.net'  
option interface    'sixxs.0'  
option tunnel_id    'Txxxx'  
option requiretls   ''  
option defaultroute '1'  
option nat          '0'  
option heartbeat    '1'
```

IPv6 via Tunnel zu ISP SixXS Aktivierung



♦ Autostart

```
# /etc/init.d/aiccu enable
```

♦ Aktivierung

```
# /etc/init.d/aiccu start
```

♦ Logging

```
gate6pbg syslog: Succesfully retrieved tunnel information for Txxxx
```

```
gate6pbg syslog: AICCU running as PID 15532
```

```
gate6pbg kernel: sixxs.0: Disabled Privacy Extensions
```

```
gate6pbg firewall: adding wan6 (sixxs.0) to zone wan
```

```
gate6pbg firewall: removing wan6 (sixxs.0) from zone wan
```

```
gate6pbg firewall: adding wan6 (sixxs.0) to zone wan
```

IPv6 via Tunnel zu ISP SixXS Test



◆ Tunnelschnittstelle nach erfolgreichem Aufbau

```
# ifconfig sixxs.0
```

```
sixxs.0 Link encap:IPv6-in-IPv4  
inet6 addr: 2001:6f8:900:449::2/64 Scope:Global  
inet6 addr: fe80::ac10:1101/64 Scope:Link  
inet6 addr: fe80::bcae:3a20/64 Scope:Link  
inet6 addr: fe80::c0a8:1101/64 Scope:Link  
UP POINTOPOINT RUNNING NOARP MTU:1280 Metric:1  
...
```

```
# ping6 -c 1 www.ipv6.bieringer.de
```

```
PING www.ipv6.bieringer.de (2001:4dd0:f838:a006::6): 56 data bytes  
64 bytes from 2001:4dd0:f838:a006::6: seq=0 ttl=52 time=56.198 ms
```

Zugang via gogo6

IPv6 via Tunnel zu ISP gogo6 Installation



- ▶ **Nur authentifizierter Zugang sinnvoll**

- ◆ Statische IPv6-Adresse
- ◆ Zuweisung /56 IPv6-Subnetz

- ▶ **“ip” installieren (Abhängigkeiten)**

```
# opkg install ip
```

- ▶ **Tunnel-Programm “aiccu” installieren**

```
# opkg install gw6c
```

IPv6 via Tunnel zu ISP gogo6 Konfiguration



◆ Konfigurationsdatei: /etc/config/gw6c

```
config gw6c basic
    option disabled 0
    option userid 'USER'
    option passwd 'PASSWORD'
    option server broker.freenet6.net
    option auth_method any

config gw6c routing
    option host_type router
    option prefixlen 56
    option ifprefix br-lan

config gw6c logging
    option log_console 0
    option log_stderr 0
    option log_file 0
    option log_syslog 1
```

IPv6 via Tunnel zu ISP gogo6 Aktivierung



▶ Autostart

```
# /etc/init.d/gw6c enable
```

▶ Aktivierung

```
# /etc/init.d/gw6c start
```

```
gw6c: Gateway6 Client v5.1-RELEASE build Nov 16 2011-01:45:53
```

```
gw6c: Built on ///Linux nd-build-02.linux-appliance.net 2.6.18-238.19.1.el5PAE  
#1 SMP Fri Jul 15 08:15:44 EDT 2011 i686 i686 i386 GNU/Linux///
```

```
gw6c: Received a TSP redirection message from Gateway6 broker.freenet6.net  
(1200 Redirection#015).
```

```
gw6c: The Gateway6 redirection list is [ sydney.freenet6.net, amster-  
dam.freenet6.net, montreal.freenet6.net ].
```

```
gw6c: The optimized Gateway6 redirection list is [ amsterdam.freenet6.net,  
montreal.freenet6.net, sydney.freenet6.net ].
```

```
gw6c: Connection to amsterdam.freenet6.net established.
```

IPv6 via Tunnel zu ISP gogo6 Test



◆ Schnittstellen nach erfolgreichem Aufbau

```
# ifconfig sit1
```

```
sit1      Link encap:IPv6-in-IPv4  
          inet6 addr: 2001:5c0:1400:a:8000:0:5801:2345/128 Scope:Global  
          inet6 addr: fe80::ac10:1101/64 Scope:Link  
          inet6 addr: fe80::5801:2345/64 Scope:Link  
          inet6 addr: fe80::c0a8:1101/64 Scope:Link  
          UP POINTOPOINT RUNNING NOARP MTU:1280 Metric:1
```

```
# ifconfig br-lan
```

```
br-lan    Link encap:Ethernet HWaddr 00:12:17:01:23:45  
          inet addr:192.168.17.1 Bcast:192.168.17.255 Mask:255.255.255.0  
          inet6 addr: 2001:5c0:1500:0000::1/64 Scope:Global  
          inet6 addr: fe80::212:17ff:fe01:2345/64 Scope:Link  
          UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
```

◆ Test

```
# ping6 -c 1 www.ipv6.bieringer.de
```

```
PING www.ipv6.bieringer.de (2001:4dd0:f838:a006::6): 56 data bytes  
64 bytes from 2001:4dd0:f838:a006::6: seq=0 ttl=52 time=56.198 ms
```

Absicherung & Firewalling

Absicherung & Firewalling

Gefährdete offene Ports

◆ Standardinstallation

```
# netstat -nlptu
```

```
Active Internet connections (only servers)
```

Proto	Recv-Q	Send-Q	Local Address	Foreign Address	State	PID/Program name
tcp	0	0	0.0.0.0:80	0.0.0.0:*	LISTEN	1274/uhttpd
tcp	0	0	0.0.0.0:53	0.0.0.0:*	LISTEN	15931/dnsmasq
tcp	0	0	:::53	:::*	LISTEN	15931/dnsmasq
tcp	0	0	:::22	:::*	LISTEN	1265/dropbear
udp	0	0	0.0.0.0:47887	0.0.0.0:*		334/syslogd
udp	0	0	0.0.0.0:53	0.0.0.0:*		15931/dnsmasq
udp	0	0	0.0.0.0:67	0.0.0.0:*		15931/dnsmasq
udp	0	0	:::53	:::*		15931/dnsmasq

Absicherung notwendig!

IPv4 & IPv6: SSH via “dropbear” (22/tcp)

Absicherungsmöglichkeiten

◆ SSH (via “dropbear”)

- ◆ Mindestens Port verstellen!
 - ◆ Datei: /etc/config/dropbear

```
config 'dropbear'
```

```
option 'Port' '12345'
```

- ◆ Authentifizierung via Passwort abstellen

◆ Eingebaute Firewall

- ◆ Standardmäßig aktiv
- ◆ Ggf. Regelwerkprüfung notwendig

Eingebaute Firewall

- ▶ **Unterstützt IPv4 & IPv6 (abb 10.03.1)**
- ▶ **Zonenbasiert**
 - ◆ Standardzonen: Device, LAN, WAN
 - ◆ Eigene weitere Zonen möglich (z.B. GAST)
 - ◆ Schnittstellen können Zonen zugewiesen werden
- ▶ **Administrierbar via**
 - ◆ WebUI (LuCI)
 - ◆ CLI
 - ◆ Datei: /etc/config/firewall (Firewallregeln)
 - ◆ Datei: /etc/config/network (Schnittstellen)

Eingebaute Firewall Interfaces (1)

The screenshot shows the OpenWRT web interface with the 'Network' tab selected. The 'Interfaces' sub-tab is active, displaying a list of network interfaces. The interface 'WANGOGO6' is highlighted in red, indicating it is the selected interface. The table below provides details for each interface, including its name, status, MAC address, and IP configuration. The 'Actions' column for each interface contains buttons for 'Connect', 'Stop', 'Edit', and 'Delete'.

Network	Status	Actions
WANGOGO6 sit1	IPv6 via gogo6 MAC Address: 00:00:00:00:00:00 RX: 0.00 B (0 Pkts.) TX: 0.00 B (0 Pkts.)	Connect Stop Edit Delete
GUEST br-guest	Uptime: 0h 54m 55s MAC Address: 00:12:17:07:B9:DC RX: 0.00 B (0 Pkts.) TX: 1.08 KB (8 Pkts.) IPv4: 172.16.17.1/24 IPv6: FE80:0:0:0:212:17FF:FE[REDACTED]/64	Connect Stop Edit Delete
LAN br-lan	Uptime: 0h 55m 19s MAC Address: 00:12:17:07:B9:DC RX: 3.21 MB (50703 Pkts.) TX: 87.24 MB (64840 Pkts.) IPv4: 192.168.17.1/24 IPv6: 2001:5C0:15[REDACTED]:0:0:0:1/64, FE80:0:0:0:212:17FF:FE[REDACTED]	Connect Stop Edit Delete
WAN pppoe-wan	IPv4 Uptime: 0h 55m 15s RX: 84.20 MB (57093 Pkts.) TX: 2.33 MB (41106 Pkts.) IPv4: 188.174.201.219/32	Connect Stop Edit Delete
WAN6 sixxs-0	IPv6 via SixXS MAC Address: 00:00:00:00:00:00 RX: 0.00 B (0 Pkts.) TX: 0.00 B (0 Pkts.)	Connect Stop Edit Delete

[Add new interface...](#)

Eingebaute Firewall Interfaces (2)

◆ Datei: /etc/config/network (Auszug)

```
config 'interface'          'wan6'  
    option 'proto'          'none'  
    option 'ifname'         'sixxs.0'  
  
config 'interface'          'WANGogo6'  
    option 'proto'          'none'  
    option 'ifname'         'sit1'
```

Eingebaute Firewall Zonen (1)

Firewall

The firewall creates zones over your network interfaces to control network traffic flow.

General Settings | Custom Rules

Enable SYN-flood protection

Drop invalid packets

Input: accept

Output: accept

Forward: reject

Zones

Zone ⇒ Forwardings	Input	Output	Forward	Masquerading	MSS clamping	
lan: lan: ⇒ wan	accept	accept	reject	<input type="checkbox"/>	<input type="checkbox"/>	
wan: WANgogo6: wan: wan6: ⇒ REJECT	reject	accept	reject	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
guest: guest: ⇒ REJECT	accept	accept	reject	<input type="checkbox"/>	<input type="checkbox"/>	

Add

Eingebaute Firewall

Zonen (2)

The screenshot shows the OpenWRT web interface for configuring the 'wan' firewall zone. The page is titled 'Firewall - Zone Settings' and has a navigation bar with tabs for Status, System, Services, Network, and Logout. Under the Network tab, there are sub-tabs for Interfaces, Wifi, Switch, DHCP and DNS, Hostnames, Static Routes, Diagnostics, Firewall, and Radvd. The 'Firewall' sub-tab is active.

Zone "wan"

This section defines common properties of "wan". The *input* and *output* options set the default policies for traffic entering and leaving this zone while the *forward* option describes the policy for forwarded traffic between different networks within the zone. *Covered networks* specifies which available networks are member of this zone.

General Settings | **Advanced Settings**

Name	wan
Input	reject
Output	accept
Forward	reject
Masquerading	<input checked="" type="checkbox"/>
MSS clamping	<input checked="" type="checkbox"/>
Covered networks	<input checked="" type="checkbox"/> WANgogo6: <input type="checkbox"/> guest: <input type="checkbox"/> lan: <input checked="" type="checkbox"/> wan: <input checked="" type="checkbox"/> wan6:

Inter-Zone Forwarding

The options below control the forwarding policies between this zone (wan) and other zones. *Destination zones* cover forwarded traffic **originating from "wan"**. *Source zones* match forwarded traffic from other zones **targeted at "wan"**. The forwarding rule is *unidirectional*, e.g. a forward from lan to wan does *not* imply a permission to forward from wan to lan as well.

Allow forward to <i>destination zones</i> :	<input type="checkbox"/> guest:
	<input type="checkbox"/> lan:
Allow forward from <i>source zones</i> :	<input type="checkbox"/> guest:
	<input checked="" type="checkbox"/> lan:

Eingebaute Firewall Zonen (3)





















- **Datei: /etc/config/firewall (Beispiele)**


```
config 'zone'  
    option 'name'          'lan'  
    option 'network'      'lan'  
    option 'input'        'ACCEPT'  
    option 'output'       'ACCEPT'  
    option 'forward'     'REJECT'
```




```
config 'zone'  
    option 'name'          'wan'  
    option 'input'        'REJECT'  
    option 'output'       'ACCEPT'  
    option 'forward'     'REJECT'  
    option 'masq'         '1'  
    option 'mtu_fix'      '1'  
    option 'network'     'WANgogo wan wan6'
```

Eingebaute Firewall Regeln (1)

Rules

Name	Family	Protocol	Source	Destination	Action	Sort	
WAN-DEVICE-ICMPv4-Accept	IPv4 only	ICMP (echo-request)	wan:0.0.0.0/0.*	Device:0.0.0.0/0.*	ACCEPT	↑ ↓	 
WAN-DEVICE-DHCPv6-Reply-Accept	IPv6 only	UDP	wan:fe80::/10:547	Device:fe80::/10:546	ACCEPT	↑ ↓	 
WAN-DEVICE-ICMPv6-Accept	IPv6 only	ICMP (echo-request)	wan:0.0.0.0/0.*	Device:0.0.0.0/0.*	ACCEPT	↑ ↓	 
WAN-LAN-ICMPv6-Accept	IPv6 only	ICMP (echo-request)	wan:0.0.0.0/0.*	lan:0.0.0.0/0.*	ACCEPT	↑ ↓	 
LAN-WAN-ICMP-Accept	IPv4 and IPv6	ICMP	lan:0.0.0.0/0.*	wan:0.0.0.0/0.*	ACCEPT	↑ ↓	 
LAN-WAN-NTP-Accept	IPv4 and IPv6	UDP	lan:0.0.0.0/0.*	wan:0.0.0.0/0:123	ACCEPT	↑ ↓	 
LAN-WAN-DNS-Accept	IPv4 and IPv6	TCP+UDP	lan:0.0.0.0/0.*	wan:0.0.0.0/0:53	ACCEPT	↑ ↓	 
LAN-WAN-HTTP-Accept	IPv4 and IPv6	TCP	lan:0.0.0.0/0.*	wan:0.0.0.0/0:80	ACCEPT	↑ ↓	 
LAN-WAN-HTTPS-Accept	IPv4 and IPv6	TCP	lan:0.0.0.0/0.*	wan:0.0.0.0/0:443	ACCEPT	↑ ↓	 
LAN-WAN-FTP-Accept	IPv4 and IPv6	TCP	lan:0.0.0.0/0.*	wan:0.0.0.0/0:21	ACCEPT	↑ ↓	 

 Add

 Reset  Save  Save & Apply

Eingebaute Firewall Regeln (2)

◆ Datei: /etc/config/firewall (Beispiele)

◆ Regel für stateless DHCPv6

```
config 'rule'  
    option 'src'          'wan'  
    option 'proto'        'udp'  
    option 'src_ip'       'fe80::/10'  
    option 'src_port'     '547'  
    option 'dest_ip'      'fe80::/10'  
    option 'dest_port'    '546'  
    option 'family'       'ipv6'  
    option 'target'       'ACCEPT'  
    option 'name'         'Allow-DHCPv6'  
    option '_name'        'WAN-DEVICE-DHCPv6-Reply-Accept'
```

◆ Regel für ausgehendes HTTP

```
config 'rule'  
    option 'src'          'lan'  
    option 'dest'         'wan'  
    option 'proto'        'tcp'  
    option 'dest_port'    '80'  
    option 'target'       'ACCEPT'  
    option '_name'        'LAN-WAN-HTTP-Accept'
```

Fehlersuche

Fehlersuche

- ◆ **syslog**
- ◆ **tcpdump**
- ◆ **iptables / ip6tables**

Weitere Informationen

IPv6 & Linux bezogene Information

- ◆ ***OpenWRT IPv6 HOWTO***

 - ◆ <http://wiki.openwrt.org/doc/howto/ipv6>

- ◆ ***SixXS / aiccu / OpenWRT***

 - ◆ https://www.sixxs.net/wiki/Aiccu/Installing_on_OpenWRT

Kontakt-Information

peter@deepspace6.net

<http://www.deepspace6.net/>



pb@bieringer.de

<http://www.bieringer.de/pb/>

<http://www.bieringer.de/linux/IPv6/>

<http://mirrors.bieringer.de/>

Vielen Dank für die Teilnahme!

Fragen & Antworten

Tutorial mit Notizen ist als PDF per E-Mail bzw. über Veranstalter erhältlich!

Dankeschön an

Jürgen Seeger, iX & Johannes Endres, c't (Einladung)

IPv6 mit OpenWRT (Einführung)

Tutorial

Dr. Peter Bieringer
Deep Space 6
peter@deepspace6.net
<http://www.deepspace6.net/>



IPv6-Kongress
Frankfurt/Main, Deutschland
10. - 11. Mai 2012
<http://www.ipv6-kongress.de/>

Inhalt

IPv6 mit OpenWRT (Einführung)

- ♦ **Allgemeines**
- ♦ **Voraussetzungen & Empfehlungen**
- ♦ **IPv6-Konfiguration**
- ♦ **IPv6-Anbindungen**
 - ♦ PPPv6 & DHCPv6
 - ♦ SixXS
 - ♦ gogo6
- ♦ **Absicherung & Firewalling**
- ♦ **Fehlersuche**

Allgemeines zu OpenWRT

Allgemeines zu OpenWRT

- ◆ **OpenWRT basiert auf Linux**
- ◆ **Schnittstellen**
 - ◆ Interne Schnittstellen üblicherweise als Linux-Bridges definiert
 - ◆ Z.B: br-lan, br-guest
 - ◆ Externe Schnittstelle (“Uplink”) u.a.
 - ◆ PPPoE
 - ◆ DHCPv4
 - ◆ Statisch
- ◆ **Administration**
 - ◆ Web-Oberfläche
 - ◆ Via SSH und Konfigurationsdateien

Voraussetzungen für IPv6 in OpenWRT

IPv6 in OpenWRT

Voraussetzungen - Version

- ◆ **Welche Version?**
 - ◆ IPv6-Unterstützung seit *Kamikaze Version 7*
 - ◆ Empfohlen: *Backfire Version 10.03.1*
 - ◆ Aktuelle Version!
 - ◆ IPv6-Unterstützung der Firewall brauchbar!

IPv6 in OpenWRT

Voraussetzungen - Basis

♦ IPv6-Kernelmodul installiert?

♦ Test

```
# opkg list_installed | grep kmod-ipv6  
kmod-ipv6 - 2.6.32.27-1
```

♦ Installation

```
# opkg update  
# opkg install kmod-ipv6
```

♦ IPv6 Kernelmodul aktiv?

♦ Test

```
# wc -l /proc/net/if_inet6  
29 /proc/net/if_inet6
```

IPv6 in OpenWRT

Voraussetzungen - Erweiterung

♦ Router Advertisement -Programm “radvd”

♦ Installation

```
# opkg install radvd
```

♦ IPv6-Firewall-Erweiterung installiert?

♦ Installation

```
# opkg install kmod-ip6tables ip6tables
```

Empfehlungen (nicht nur) für IPv6 in OpenWRT

IPv6 in OpenWRT

Empfehlungen

♦ Remote-Syslog aktivieren

♦ Sehr hilfreich für Debugging on-the-fly

♦ Syslog-Konfiguration

♦ Datei: /etc/config/system

```
config 'system'
    option 'log_ip' '192.168.1.2'
```

♦ Syslog-Ziel:

♦ Konfiguration für z.B. rsyslog:

```
♦ Datei: /etc/rsyslog.d/openwrt.conf
    :fromhost-ip, isequal, "192.168.1.1" /var/log/openwrt
    & ~
```

♦ Ggf. logrotate-Konfiguration erweitern

♦ Beispielkonfiguration: siehe Notizen

Aktivieren des Empfangs von Remote-Syslog-Paketen

Datei: /etc/rsyslog.conf

```
# Provides UDP syslog reception
$ModLoad imudp
$UDPServerRun 514
```

Restart:

```
# service rsyslog restart
```

Firewall

Empfang von Remote-Syslog-Paketen (eingeschränkt auf eine Quell-IP)

```
# iptables -I INPUT -p udp -s 192.168.1.1 --dport 514 -j ACCEPT
```

Logrotation (verhindert das Überlaufen des Dateisystems)

Datei: /etc/logrotate.d/openwrt

```
/var/log/openwrt {
    sharedscripts
    postrotate
        /bin/kill -HUP `cat /var/run/syslogd.pid 2> /dev/null` 2> /dev/null || true
    endscript
}
```

Test von OpenWRT aus

Auslösen von Syslog-Events

```
# logger test
# logger -p debug testdebug
```

IPv6-Konfiguration von OpenWRT

IPv6-Konfiguration

- ◆ **Statisch**
 - ◆ IPv6-Adresse
 - ◆ Routing
 - ◆ Router-Advertisements

IPv6-Adresskonfiguration

Ansicht

♦ Werkzeuge `ifconfig`

- ♦ oder `ip` (muß erst installiert werden)

```
# ifconfig INTERFACE
```

```
# ip -6 addr show dev INTERFACE
```

♦ Beispiele

```
# ifconfig br-lan
```

```
br-lan    Link encap:Ethernet  HWaddr 00:12:17:01:23:45
          inet addr:192.168.17.1  Bcast:192.168.17.255  Mask:255.255.255.0
          inet6 addr: 2001:6f8:133d:1::1/64  Scope:Global
          inet6 addr: fe80::212:17ff:fe01:2345/64  Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:360447 errors:0 dropped:0 overruns:0 frame:0
          TX packets:254666 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:58867265 (56.1 MiB)  TX bytes:230469793 (219.7 MiB)
```

Dr. Peter Bieringer – IPv6 mit OpenWRT (Tutorial) – IPv6-Kongress – 10. -11. Mai 2012, Frankfurt/Main, Deutschland 11.05.12 13:46:30 13

Werkzeug: `ip`

```
# ip addr show dev br-lan
```

```
6: br-lan: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UNKNOWN
    link/ether 00:12:17:01:23:45 brd ff:ff:ff:ff:ff:ff
    inet 192.168.17.1/24 brd 192.168.17.255 scope global br-lan
    inet6 2001:6f8:133d:1::1/64 scope global
        valid_lft forever preferred_lft forever
    inet6 fe80::212:17ff:fe01:2345/64 scope link
        valid_lft forever preferred_lft forever
```

IPv6-Adresskonfiguration

Statische Zuweisung (1)

♦ Konfigurationsdatei: /etc/config/network

```
config 'interface' 'lan'  
    option 'type' 'bridge'  
    option 'ifname' 'eth0.0'  
    option 'proto' 'static'  
    option 'netmask' '255.255.255.0'  
    option 'ipaddr' '192.168.17.1'  
    option 'ip6addr' '2001:6f8:133d:1::1/64'
```

IPv6-Adresskonfiguration

Statische Zuweisung (2)

The screenshot shows the OpenWRT web interface for configuring the LAN interface. The page title is "Interfaces - LAN". Below the title, there is a status box with the following information:

- Uptime: 22d 17h 17m 13s
- MAC Address: 00:12:17:07:B9:DC
- RX: 59.09 MB (362124 Pkts)
- TX: 230.70 MB (256888 Pkts)
- IPv4: 192.168.17.124
- IPv6: 2001:6f8:133d:1:0:0:164, FE80:0:0:212:17FF:FE[redacted]/64

The configuration table below shows the following settings:

Field	Value
Protocol	Static address
IPv4 address	192.168.17.1
IPv4 netmask	255.255.255.0
IPv4 gateway	
IPv4 broadcast	
Use custom DNS servers	
Accept router advertisements	<input type="checkbox"/>
Send router solicitations	<input checked="" type="checkbox"/>
IPv6 address	2001:6f8:133d:1::1/64
IPv6 gateway	

IPv6-Routing Ansicht

♦ Werkzeuge route

- ♦ oder ip (muß erst installiert werden)

```
# route -n -A inet6
# ip -6 route show [dev INTERFACE]
```

♦ Beispiele

```
# route -n -A inet6 | grep br-lan
2001:6f8:133d:1::/64      ::          U          256        0          0 br-lan
fe80::/64                ::          U          256        0          0 br-lan
ff00::/8                 ::          U          256        0          0 br-lan
```

Werkzeug: ip

```
# ip -6 route
```

```
2001:6f8:133d:1::/64 dev br-lan proto kernel metric 256 mtu 1500 advmss 1440 hoplimit 0
```

```
fe80::/64 dev eth0 proto kernel metric 256 mtu 1500 advmss 1440 hoplimit 0
```

```
fe80::/64 dev br-lan proto kernel metric 256 mtu 1500 advmss 1440 hoplimit 0
```

```
fe80::/64 dev eth0.1 proto kernel metric 256 mtu 1500 advmss 1440 hoplimit 0
```

```
fe80::/64 dev br-guest proto kernel metric 256 mtu 1500 advmss 1440 hoplimit 0
```

IPv6-Routing Konfiguration (1)

♦ Konfigurationsdatei: /etc/config/network

```
config 'route6'  
    option 'interface' 'lan'  
    option 'target' 'fec0:0:0:2::/64'  
    option 'gateway' 'fec0:0:0:1::2/64'
```

IPv6-Routing Konfiguration (2)

The screenshot shows the OpenWRT web interface for configuring static IPv6 routes. The page title is "Routes" and it includes a sub-header "Static IPv6 Routes". The configuration table is as follows:

Interface	Target <small>IPv6-Address or Network (CIDR)</small>	IPv6-Gateway	Metric	MTU
lan	fec0:0:0:2::/64	fec0:0:0:1::2/64	0	1500

At the bottom of the configuration area, there are buttons for "Reset", "Save", and "Save & Apply".

IPv6-Adresskonfiguration Router Advertisements (1)

◆ Konfigurationsdatei: /etc/config/radvd

```
config 'interface'
    option 'interface' 'lan'
    option 'AdvSendAdvert' '0'
    option 'IgnoreIfMissing' '1'
    option 'AdvSourceLLAddress' '1'
    option 'AdvDefaultPreference' 'medium'
    option 'MinRtrAdvInterval' '30'
    option 'MaxRtrAdvInterval' '120'

config 'prefix'
    option 'ignore' '0'
    option 'interface' 'lan'
    option 'AdvOnLink' '1'
    option 'AdvAutonomous' '1'
    list 'prefix' '2001:6f8:133d:0001::/64'
```


IPv6-Adresskonfiguration Router Advertisements (2)

gate6ppbg | OpenWRT Backfire 10.03.1 | Load: 0.37 0.35 0.15 Changes: 0

Status System Services **Network** Logout

Interfaces Wifi Switch DHCP and DNS Hostnames Static Routes Diagnostics Firewall **Radvd**

Radvd

Radvd is a router advertisement daemon for IPv6. It listens to router solicitations and sends router advertisements as described in RFC 4861.

Interfaces

Enable	Interface	Multicast	Advertising	Max. interval	Mobile IPv6	Preference
<input checked="" type="checkbox"/>	lan:	<input checked="" type="radio"/>	<input type="checkbox"/>	120s	<input type="checkbox"/>	medium

[Add](#)

Prefixes

Enable	Interface	Prefix	Autonomous On-link Validity time
<input checked="" type="checkbox"/>	lan:	2001:6f8:133d:1:0:0:0:1/64	<input checked="" type="checkbox"/>

[Add](#)

Routes

Enable	Interface	Prefix	Lifetime	Preference
<input type="checkbox"/>	lan:	2001:6f8:133d:1:0:0:0:1/64	1800	medium

[Add](#)

RDNSS

Enable	Interface	Address	Lifetime
<input type="checkbox"/>	lan:	2001:6f8:133d:1:0:0:0:1/64	1200

[Add](#)

DISSL

Enable	Interface	Suffix	Lifetime
<input type="checkbox"/>	lan:	?	1200

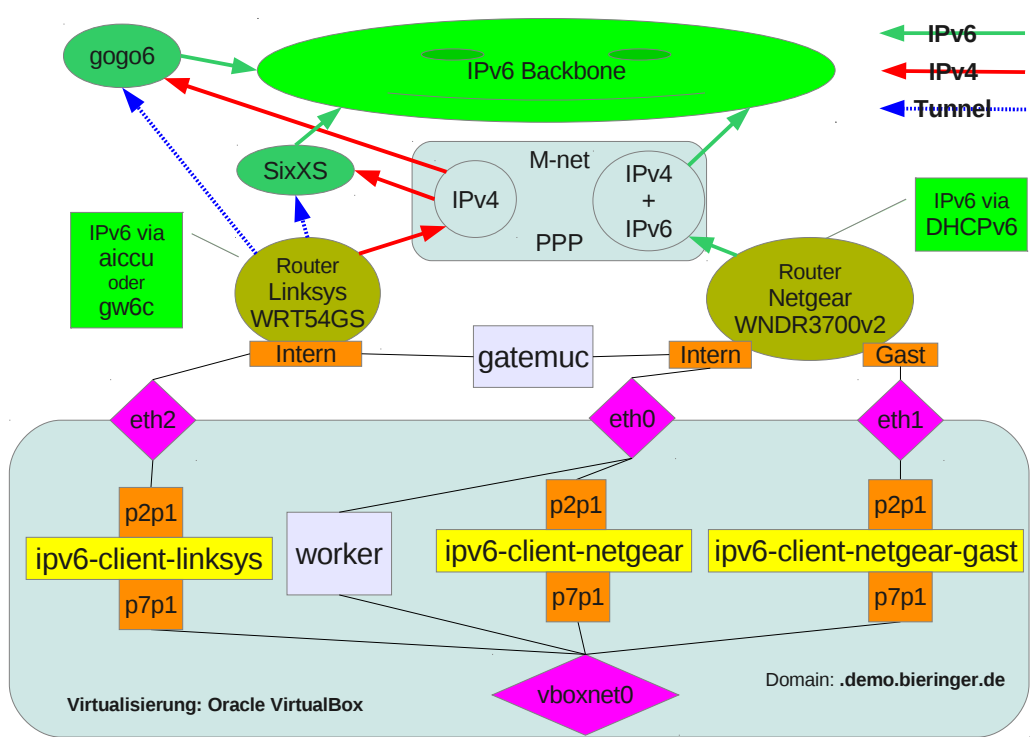
[Add](#)

IPv6-Anbindungen

IPv6-Anbindungen

- ♦ **PPPo6 & DHCPv6**
- ♦ **Tunnel via SixXS**
- ♦ **Tunnel via gogo6**

Aufbau Demonstration



Zugang via PPPv6 & DHCPv6

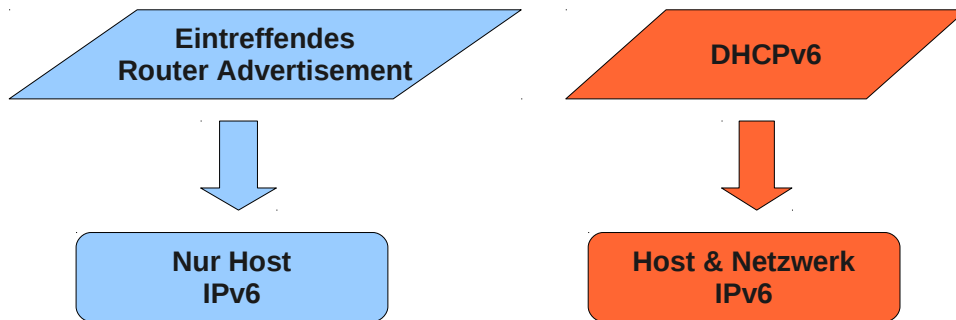
PPP für IPv6

- ♦ **PPPo6 ist definiert in RFC 5072 (ex 2472)**

- ♦ NUR Aushandlung beidseitiger link-local-Adressen
- ♦ KEINE explizite Präfix- bzw. globale Adress-Aushandlung



- ♦ Ohne Zusatzprotokolle keine globale IPv6-Kommunikation



DHCP für IPv6

◆ DHCPv6 definiert in RFC 3315

- ◆ Arbeitet mit link-local-Adressen
- ◆ Wichtige Option: DHCPv6 Präfix-Delegation (RFC 3633)
- ◆ DHCP-Server
 - ◆ Port: udp/547
- ◆ Client
 - ◆ Adresse: link-local
 - ◆ Port: udp/546 (source-port bind)
 - ◆ Ziel: ff02::1:2 (Multicast: alle DHCP-Agenten am Link)



- ◆ Probleme mit Stateful Firewall durch zusätzliche Regeln lösen
 - ◆ Client & Client: stateless

PPP / DHCP für IPv6

◆ **“Connect”**

- ◆ Startet PPP (oder PPPoE)
 - ◆ PPPv6: Handelt link-local Adresse aus
- ◆ Startet DHCPv6 Client
 - ◆ Client sendet DHCPv6-Anfrage incl. Präfix-Anfrage
 - ◆ Server sendet DHCPv6-Antwort samt Präfix
 - ◆ Client konfiguriert ein oder mehrere Schnittstellen abhängig von lokal vorher definierten SLA
- ◆ Client (re-)startet Router Advertisement Daemon mit neuen Präfixes

Adresszuweisung via DHCPv6

♦ Generell

TLD	NLA	SLA	IID 64
-----	-----	-----	-----------

♦ M-net (München)

2001:0a60::/32 DE-MNET 32	2001:0a60:1000::/37 RESIDENTIAL-MUC 5	Zugänge München 19	SLA 8	IID 64
56				



Präfix via
DHCPv6



Lokale
Konfiguration

IPv6 nativ via PPPv6 & DHCPv6



♦ ISP: M-net

- ♦ IPv4: IPv6-Präfix für PPP-Schnittstelle via RA
 - ♦ PPP-Benutzer: Xxxxxx@**mdsl**.mnet-online.de'
- ♦ IPv6-Test: via DHCPv6
 - ♦ PPP-Benutzer: Xxxxxx@**v6**.mnet-online.de'

♦ OpenWRT-Konfiguration

- ♦ IPv6 aktiv für WAN-Schnittstelle
 - ♦ "Enable IPv6 negotiation on the PPP link"
- ♦ DHCPv6 konfiguriert
 - ♦ CLI-Konfiguration notwendig
- ♦ Radvd konfiguriert
 - ♦ Mit generischem Präfix den jeweilig zugewiesenen verteilen
 - ♦ Präfix: 0:0:0:0:0:0:0:0/64

IPv6 nativ via PPPv6 & DHCPv6

♦ Funktionsweise in OpenWRT

- ♦ Herstellung PPP-Verbindung
- ♦ Starten von dhcp6c via Hotplug
 - ♦ IPv6-Präfix von ISP via DHCPv6
 - ♦ Präfix + konfigurierter SLA pro Schnittstelle => Adresse zuweisen
 - ♦ Restart von Radvd via Hotplug

IPv6 nativ via PPPv6 & DHCPv6 Installation

- ♦ Paket “dhcp6-client” fehlen Hotplug-Skripte
- ♦ Paket “wide-dhcp6c-client” installieren

```
# opkg install wide-dhcpv6-client
```

IPv6 nativ via PPPv6 & DHCPv6 Konfiguration RADVD

- ▶ **Später via DHCPv6 zugewiesener Präfix durch den ISP nicht bekannt**
 - ▶ Spezialkonfiguration für RADVD notwendig
 - ▶ Spezial-Präfix: `::/64` pro Schnittstelle
 - ▶ RADVD konfiguriert bei "reload" pro definierter Schnittstelle automatisch von JEDER existierenden IPv6-Adresse

- ▶ **Konfigurationsdatei: `/etc/config/radvd`**

```
config 'prefix'  
    option 'ignore'          '0'  
    option 'interface'      'lan'  
    option 'AdvOnLink'      '1'  
    option 'AdvAutonomous'  '1'  
    list 'prefix'           '::/64'
```

IPv6 nativ via PPPv6 & DHCPv6

Konfiguration PPPv6 (1)

- ◆ Konfiguration über WebUI oder CLI möglich

- ◆ Datei: /etc/config/network

```
config 'interface' 'wan'  
  option '_orig_ifname' 'eth1'  
  option '_orig_bridge' 'false'  
  option 'proto' 'pppoe'  
  option 'password' 'SECRET'  
  option 'ipv6' '1'  
  option 'ifname' 'eth1'  
  option 'username' 'XA.....@v6.mnet-online.de'
```

IPv6 nativ via PPPv6 & DHCPv6 Konfiguration PPPv6 (2)

The screenshot shows the OpenWRT web interface for configuring the WAN interface. The browser address bar shows 'gate6muc.muc.bieringer.de | OpenWrt Backfire 10.03.1 | Load: 0.00 0.10 0.10 | Auto Refresh: on'. The navigation menu includes 'Status', 'System', 'Services', 'Network', and 'Logout'. Under 'Network', there are sub-menus for 'Interfaces', 'Wifi', 'Switch', 'DHCP and DNS', 'Hostnames', 'Static Routes', 'Diagnostics', 'Firewall', and 'Radvd'. The 'Interfaces' menu is selected, and the 'WAN' tab is active. The page title is 'Interfaces - WAN'. Below the title, there is a brief instruction: 'On this page you can configure the network interfaces. You can bridge several interfaces by ticking the "bridge interfaces" field and enter the names of several network interfaces separated by spaces. You can also use VLAN notation INTERFACE.VLANNR (e.g.: eth0.1)'. The main configuration area is titled 'Common Configuration' and has four tabs: 'General Setup', 'Advanced Settings', 'Physical Settings', and 'Firewall Settings'. The 'General Setup' tab is selected. The configuration options are as follows:

Bring up on boot	<input checked="" type="checkbox"/>	
Enable IPv6 negotiation on the PPP link	<input checked="" type="checkbox"/>	
Use default gateway	<input checked="" type="checkbox"/>	If unchecked, no default route is configured
Use gateway metric	<input type="text" value="0"/>	
Use DNS servers advertised by peer	<input checked="" type="checkbox"/>	If unchecked, the advertised DNS server addresses are ignored
LCP echo failure threshold	<input type="text" value="0"/>	Presume peer to be dead after given amount of LCP echo failures, use 0 to ignore failures
LCP echo interval	<input type="text" value="5"/>	Send LCP echo requests at the given interval in seconds, only effective in conjunction with failure threshold
Inactivity timeout	<input type="text" value="0"/>	Close inactive connection after the given amount of seconds, use 0 to persist connection

IPv6 nativ via PPPv6 & DHCPv6

Aktivierung PPPv6

♦ (Re-)Connect der WAN-Schnittstelle (oder Reboot)

```
# kill -SIGHUP `pidof pppd`
```

♦ Logging (Auszug)

```
pppd: Connect: pppoe-wan <-> eth1  
pppd: primary DNS address 212.18.0.5  
pppd: secondary DNS address 212.18.3.5  
pppd: local LL address fe80::ac92:0102:d101:2345  
pppd: remote LL address fe80::0090:1a00:0201:2345
```


IPv6 nativ via PPPv6 & DHCPv6

Test PPPv6

♦ PPP-Schnittstelle nach erfolgter Einwahl

```
# ifconfig pppoe-wan
pppoe-wan Link encap:Point-to-Point Protocol
      inet addr:93.104.1.1  P-t-P:82.135.1.1  Mask:255.255.255.255
      inet6 addr: fe80::f105:52d3:fe01:2345/10 Scope:Link
      UP POINTOPOINT RUNNING NOARP MULTICAST MTU:1492 Metric:1
```


♦ Test

```
# ping6 -I pppoe-wan -c 1 fe80::0090:1a00:0201:2345
PING fe80::0090:1a00:0201:2345 (fe80::90:1a00:201:2345): 56 data bytes
64 bytes from fe80::90:1a00:201:2345: seq=0 ttl=255 time=8.487 ms

--- fe80::0090:1a00:0201:2345 ping statistics ---
1 packets transmitted, 1 packets received, 0% packet loss
round-trip min/avg/max = 8.487/8.487/8.487 ms
```

IPv6 nativ via PPPv6 & DHCPv6

Konfiguration DHCPv6 (1)

- ◆ **Konfiguration nur über CLI aktuell möglich**
 - ◆ Keine Unterstützung via WebUI “luci”
- ◆ **Konfiguration anpassen**
 - ◆ für interne Schnittstelle “br-lan”
 - ◆ für loopback-Schnittstelle “lo”
 - ◆ Router selbst bekommt damit globale IPv6-Adresse
 - ◆ Vereinfacht IPv6-Verbindungstests
 - ◆ Erreichbar von außen 
- ◆ **Logging**
 - ◆ Für erste Tests “debug” aktivieren
 - ◆ Externer Syslog-Server sehr hilfreich dabei

IPv6 nativ via PPPv6 & DHCPv6

Konfiguration DHCPv6 (2)

♦ Datei: /etc/config/dhcp6c

```
config 'dhcp6c' 'basic'
    option 'enabled' '1'
    option 'interface' 'wan' # This is the interface the DHCPv6 client will run on
    option 'pd' '1' # Prefix Delegation
    option 'rapid_commit' '1' # Rapid Commit
    option 'domain_name_servers' '1'
    option 'debug' '1'

config 'interface' 'loopback'
    option 'enabled' '1'
    option 'sla_id' '0'
    option 'sla_len' '8' # (M-net verteilt /56)

config 'interface' 'lan'
    option 'enabled' '1'
    option 'sla_id' '1'
    option 'sla_len' '8' # (M-net verteilt /56)
```

IPv6 nativ via PPPv6 & DHCPv6

Konfiguration DHCPv6 (3)

♦ Erzeugte Konfiguration: /tmp/etc/dhcp6c.conf

```
interface pppoe-wan {
    send ia-pd 0;
    send rapid-commit;
    script "/usr/bin/dhcp6c-state";
    request domain-name-servers;
};

id-assoc pd 0 {
    prefix-interface lo {
        sla-id 0;
        sla-len 8;
    };
    prefix-interface br-lan {
        sla-id 1;
        Sla-len 8;
    };
};
```

IPv6 nativ via PPPv6 & DHCPv6

Aktivierung DHCPv6

♦ (Re-)Start von DHCPv6

- ♦ auch möglich: PPP-Reconnect oder Reboot

```
# /etc/init.d/dhcp6c restart
```

♦ Logging (Auszug)

```
dhcp6c: client6_send: send solicit to ff02::1:2
dhcp6c: client6_recv: receive reply from fe80::90:1a00:201:2345 on pppoe-wan
dhcp6c: update_prefix: create a prefix 2001:a60:1201:0000::/56 pltime=1800, ...
dhcp6c: ifaddrconf: add an address 2001:a60:1201:0000:200:ff:fe00:0/64 on lo
dhcp6c: ifaddrconf: add an address 2001:a60:1201:0001:a221:b7ff:fe01:2345/64 on br-lan
dnsmasq: using nameserver 2001:a60::53:2#53
dnsmasq: using nameserver 2001:a60::53:1#53
dnsmasq: using nameserver 212.18.0.5#53
dnsmasq: using nameserver 212.18.3.5#53
```

IPv6 nativ via PPPv6 & DHCPv6 DUID Problem DHCPv6

- ▶ **DHCPv6 verwendet DUID (DHCP Unique Identifier)**
 - ▶ DHCPv4 verwendet MAC-Adresse
- ▶ **Mögliches Problem: Ableitung der DUID nicht möglich**

```
dhcp6c: starting dhcp6c
```

```
dhcp6c: Unable to derive DUID from interface 'pppoe-wan' and no valid user DUID given
```

```
dhcp6c: get_duid: DUID file corrupted
```

```
dhcp6c: client6_init: failed to get a DUID
```

- ▶ **Manuelle Definition als Lösung**
 - ▶ DUID manuell ableiten von interner **MAC-Adresse** (DUID-LL)
 - ▶ Präfix: **00:03** (DUID-LL) **00:06** (Ethernet)
 - ▶ Datei: /etc/config/dhcp6c

```
config 'dhcp6c' 'basic'
```

```
# The given value must be uppercase and globally unique!
```

```
option 'duid' '00:03:00:06:A0:21:B7:01:23:45'
```

IPv6 nativ via PPPv6 & DHCPv6

Test DHCPv6

◆ Schnittstellen nach erfolgreichem DHCPv6

```
# ifconfig lo
lo      Link encap:Local Loopback
        inet addr:127.0.0.1  Mask:255.0.0.0
        inet6 addr: ::1/128 Scope:Host
        inet6 addr: 2001:a60:1201:0000:200:ff:fe00:0/64 Scope:Global
        UP LOOPBACK RUNNING  MTU:16436  Metric:1

# ifconfig br-lan
br-lan  Link encap:Ethernet  HWaddr A0:21:B7:01:23:45
        inet addr:192.168.1.1  Bcast:192.168.1.255  Mask:255.255.255.0
        inet6 addr: 2001:a60:1201:41cb::1/64 Scope:Global
        inet6 addr: 2001:a60:1201:4101:a221:b7ff:fe01:2345/64 Scope:Global
        inet6 addr: fe80::a221:b7ff:fe01:2345/64 Scope:Link
```

◆ Test

```
# ping6 -c 1 www.ipv6.bieringer.de
PING www.ipv6.bieringer.de (2001:4dd0:f838:a006::6): 56 data bytes
64 bytes from 2001:4dd0:f838:a006::6: seq=0 ttl=52 time=56.198 ms
```



Zugang via SixXS

IPv6 via Tunnel zu ISP SixXS Installation



- ♦ **NTP-Synchronisation notwendig!**
- ♦ **“ip” installieren (Abhängigkeiten)**

```
# opkg install ip
```

- ♦ **Tunnel-Programm “aiccu” installieren**

```
# opkg install aiccu
```

IPv6 via Tunnel zu ISP SixXS Konfiguration

♦ Konfigurationsdatei: /etc/config/aiccu



```
config aiccu
    option username      'PB530-RIPE/Txxxx'
    option password      'SECRETPASSWORD'
    option protocol      'tic'
    option server        'tic.sixxs.net'
    option interface     'sixxs.0'
    option tunnel_id     'Txxxx'
    option requiret1s    ''
    option defaultroute  '1'
    option nat           '0'
    option heartbeat     '1'
```

IPv6 via Tunnel zu ISP SixXS Aktivierung



♦ Autostart

```
# /etc/init.d/aiccu enable
```

♦ Aktivierung

```
# /etc/init.d/aiccu start
```

♦ Logging

```
gate6pbg syslog: Succesfully retrieved tunnel information for Txxxx
```

```
gate6pbg syslog: AICCU running as PID 15532
```

```
gate6pbg kernel: sixxs.0: Disabled Privacy Extensions
```

```
gate6pbg firewall: adding wan6 (sixxs.0) to zone wan
```

```
gate6pbg firewall: removing wan6 (sixxs.0) from zone wan
```

```
gate6pbg firewall: adding wan6 (sixxs.0) to zone wan
```

IPv6 via Tunnel zu ISP SixXS Test

♦ Tunnelschnittstelle nach erfolgreichem Aufbau



```
# ifconfig sixxs.0
sixxs.0  Link encap:IPv6-in-IPv4
        inet6 addr: 2001:6f8:900:449::2/64 Scope:Global
        inet6 addr: fe80::ac10:1101/64 Scope:Link
        inet6 addr: fe80::bcae:3a20/64 Scope:Link
        inet6 addr: fe80::c0a8:1101/64 Scope:Link
        UP POINTOPOINT RUNNING NOARP  MTU:1280  Metric:1
        ...

# ping6 -c 1 www.ipv6.bieringer.de
PING www.ipv6.bieringer.de (2001:4dd0:f838:a006::6): 56 data bytes
64 bytes from 2001:4dd0:f838:a006::6: seq=0 ttl=52 time=56.198 ms
```



Zugang via gogo6

IPv6 via Tunnel zu ISP gogo6 Installation



- ♦ **Nur authentifizierter Zugang sinnvoll**

- ♦ Statische IPv6-Adresse
- ♦ Zuweisung /56 IPv6-Subnetz

- ♦ **“ip” installieren (Abhängigkeiten)**

```
# opkg install ip
```

- ♦ **Tunnel-Programm “aiccu” installieren**

```
# opkg install gw6c
```

IPv6 via Tunnel zu ISP gogo6 Konfiguration

♦ Konfigurationsdatei: /etc/config/gw6c



```
config gw6c basic
    option disabled 0
    option userid 'USER'
    option passwd 'PASSWORD'
    option server broker.freenet6.net
    option auth_method any

config gw6c routing
    option host_type router
    option prefixlen 56
    option ifprefix br-lan

config gw6c logging
    option log_console 0
    option log_stderr 0
    option log_file 0
    option log_syslog 1
```

IPv6 via Tunnel zu ISP gogo6 Aktivierung



♦ Autostart

```
# /etc/init.d/gw6c enable
```

♦ Aktivierung

```
# /etc/init.d/gw6c start
```

```
gw6c: Gateway6 Client v5.1-RELEASE build Nov 16 2011-01:45:53
```

```
gw6c: Built on ///Linux nd-build-02.linux-appliance.net 2.6.18-238.19.1.el5PAE  
#1 SMP Fri Jul 15 08:15:44 EDT 2011 i686 i686 i386 GNU/Linux///
```

```
gw6c: Received a TSP redirection message from Gateway6 broker.freenet6.net  
(1200 Redirection#015).
```

```
gw6c: The Gateway6 redirection list is [ sydney.freenet6.net, amster-  
dam.freenet6.net, montreal.freenet6.net ].
```

```
gw6c: The optimized Gateway6 redirection list is [ amsterdam.freenet6.net,  
montreal.freenet6.net, sydney.freenet6.net ].
```

```
gw6c: Connection to amsterdam.freenet6.net established.
```


IPv6 via Tunnel zu ISP gogo6 Test

♦ Schnittstellen nach erfolgreichem Aufbau



```
# ifconfig sit1
sit1      Link encap:IPv6-in-IPv4
          inet6 addr: 2001:5c0:1400:a:8000:0:5801:2345/128 Scope:Global
          inet6 addr: fe80::ac10:1101/64 Scope:Link
          inet6 addr: fe80::5801:2345/64 Scope:Link
          inet6 addr: fe80::c0a8:1101/64 Scope:Link
          UP POINTOPOINT RUNNING NOARP MTU:1280 Metric:1

# ifconfig br-lan
br-lan    Link encap:Ethernet HWaddr 00:12:17:01:23:45
          inet addr:192.168.17.1 Bcast:192.168.17.255 Mask:255.255.255.0
          inet6 addr: 2001:5c0:1500:0000::1/64 Scope:Global
          inet6 addr: fe80::212:17ff:fe01:2345/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
```

♦ Test

```
# ping6 -c 1 www.ipv6.bieringer.de
PING www.ipv6.bieringer.de (2001:4dd0:f838:a006::6): 56 data bytes
64 bytes from 2001:4dd0:f838:a006::6: seq=0 ttl=52 time=56.198 ms
```

Absicherung & Firewalling

Absicherung & Firewalling

Gefährdete offene Ports

♦ Standardinstallation

```
# netstat -nlptu
```

```
Active Internet connections (only servers)
```

Proto	Recv-Q	Send-Q	Local Address	Foreign Address	State	PID/Program name
tcp	0	0	0.0.0.0:80	0.0.0.0:*	LISTEN	1274/uhttpd
tcp	0	0	0.0.0.0:53	0.0.0.0:*	LISTEN	15931/dnsmasq
tcp	0	0	:::53	:::*	LISTEN	15931/dnsmasq
tcp	0	0	:::22	:::*	LISTEN	1265/dropbear
udp	0	0	0.0.0.0:47887	0.0.0.0:*		334/syslogd
udp	0	0	0.0.0.0:53	0.0.0.0:*		15931/dnsmasq
udp	0	0	0.0.0.0:67	0.0.0.0:*		15931/dnsmasq
udp	0	0	:::53	:::*		15931/dnsmasq

Absicherung notwendig!

IPv4 & IPv6: SSH via "dropbear" (22/tcp)

Absicherungsmöglichkeiten

♦ SSH (via “dropbear”)

- ♦ Mindestens Port verstellen!
- ♦ Datei: /etc/config/dropbear

```
config 'dropbear'
```

```
option 'Port' '12345'
```

- ♦ Authentifizierung via Passwort abstellen

♦ Eingebaute Firewall

- ♦ Standardmäßig aktiv
- ♦ Ggf. Regelwerkprüfung notwendig

Eingebaute Firewall

- ◆ **Unterstützt IPv4 & IPv6 (abb 10.03.1)**
- ◆ **Zonenbasiert**
 - ◆ Standardzonen: Device, LAN, WAN
 - ◆ Eigene weitere Zonen möglich (z.B. GAST)
 - ◆ Schnittstellen können Zonen zugewiesen werden
- ◆ **Administrierbar via**
 - ◆ WebUI (Luci)
 - ◆ CLI
 - ◆ Datei: /etc/config/firewall (Firewallregeln)
 - ◆ Datei: /etc/config/network (Schnittstellen)

Eingebaute Firewall Interfaces (1)

The screenshot shows the OpenWRT web interface for managing network interfaces. The main heading is 'Interfaces'. Below it, there's a sub-heading 'Interface Overview'. The interface is organized into a table with three main columns: Network, Status, and Actions.

Network	Status	Actions
WANGOGO6 st1	MAC Address: 00:00:00:00:00:00 RX: 0.00 B (0 Pkts.) TX: 0.00 B (0 Pkts.) IPv6 via gogo6	Connect Stop Edit Delete
GUEST br-guest	Uptime: 0h 54m 55s MAC Address: 00:12:17:07:B9:DC RX: 0.00 B (0 Pkts.) TX: 1.08 KB (8 Pkts.) IPv4: 172.16.17.1/24 IPv6: FE80:0:0:212:17FF:FE[redacted]:1/64	Connect Stop Edit Delete
LAN br-lan	Uptime: 0h 55m 19s MAC Address: 00:12:17:07:B9:DC RX: 3.21 MB (50703 Pkts.) TX: 87.24 MB (64840 Pkts.) IPv4: 192.168.17.1/24 IPv6: 2001:5C0:15[redacted]:0:0:0:1/64, FE80:0:0:212:17FF:FE[redacted]	Connect Stop Edit Delete
WAN pppoe-wan	Uptime: 0h 55m 15s RX: 84.20 MB (57093 Pkts.) TX: 2.33 MB (41106 Pkts.) IPv4: 188.174.201.219/32	Connect Stop Edit Delete
WAN6 sixxs.0	MAC Address: 00:00:00:00:00:00 RX: 0.00 B (0 Pkts.) TX: 0.00 B (0 Pkts.) IPv6 via SixXS	Connect Stop Edit Delete

At the bottom of the interface list, there is a button labeled 'Add new interface...'.

Eingebaute Firewall Interfaces (2)

♦ Datei: /etc/config/network (Auszug)

```
config 'interface'          'wan6'  
    option 'proto'          'none'  
    option 'ifname'         'sixxs.0'  
  
config 'interface'          'WANGogo6'  
    option 'proto'          'none'  
    option 'ifname'         'sit1'
```

Eingebaute Firewall Zonen (1)

The screenshot shows the OpenWRT Firewall configuration interface. The 'General Settings' tab is selected, and the 'Custom Rules' sub-tab is also visible. The 'General Settings' section includes the following options:

- Enable SYN-flood protection:
- Drop invalid packets:
- Input: accept
- Output: accept
- Forward: reject

The 'Zones' section displays a table of zone forwardings:

Zone	Forwardings	Input	Output	Forward	Masquerading	MSS clamping	
lan	lan: lan: ⇒ wan	accept	accept	reject	<input type="checkbox"/>	<input type="checkbox"/>	
wan	WANgogo6: wan: wan6: ⇒ REJECT	reject	accept	reject	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
guest	guest: guest: ⇒ REJECT	accept	accept	reject	<input type="checkbox"/>	<input type="checkbox"/>	

An 'Add' button is located at the bottom left of the zones table.

Eingebaute Firewall Zonen (2)

The screenshot shows the 'Firewall - Zone Settings' page for the 'wan' zone. The page is divided into two main sections: 'General Settings' and 'Inter-Zone Forwarding'.

General Settings:

- Name: wan
- Input: reject
- Output: accept
- Forward: reject
- Masquerading:
- MSS clamping:
- Covered networks:
 - WANpogo6
 - guest
 - lan
 - wan
 - wan6

Inter-Zone Forwarding:

The options below control the forwarding policies between this zone (wan) and other zones. Destination zones cover forwarded traffic originating from "wan". Source zones match forwarded traffic from other zones targeted at "wan". The forwarding rule is unidirectional, e.g. a forward from lan to wan does not imply a permission to forward from wan to lan as well.

Allow forward to destination zones:

- guest: guest
- lan: lan

Allow forward from source zones:

- guest: guest
- lan: lan

Eingebaute Firewall Zonen (3)





















- Datei: /etc/config/firewall (Beispiele)


```
config 'zone'  
  option 'name'      'lan'  
  option 'network'   'lan'  
  option 'input'     'ACCEPT'  
  option 'output'    'ACCEPT'  
  option 'forward'   'REJECT'
```




```
config 'zone'  
  option 'name'      'wan'  
  option 'input'     'REJECT'  
  option 'output'    'ACCEPT'  
  option 'forward'   'REJECT'  
  option 'masq'      '1'  
  option 'mtu_fix'   '1'  
  option 'network'   'WANgogo6 wan wan6'
```

Eingebaute Firewall Regeln (1)

Rules

Name	Family	Protocol	Source	Destination	Action	Sort	
WAN-DEVICE-ICMPv4-Accept	IPv4 only	ICMP (echo-request)	wan:0.0.0.0/0.*	Device:0.0.0.0/0.*	ACCEPT	↑ ↓	 
WAN-DEVICE-DHCPv6-Reply-Accept	IPv6 only	UDP	wan:fe80::10:547	Device:fe80::10:546	ACCEPT	↑ ↓	 
WAN-DEVICE-ICMPv4-Accept	IPv6 only	ICMP (echo-request)	wan:0.0.0.0/0.*	Device:0.0.0.0/0.*	ACCEPT	↑ ↓	 
WAN-LAN-ICMPv6-Accept	IPv6 only	ICMP (echo-request)	wan:0.0.0.0/0.*	lan:0.0.0.0/0.*	ACCEPT	↑ ↓	 
LAN-WAN-ICMP-Accept	IPv4 and IPv6	ICMP	lan:0.0.0.0/0.*	wan:0.0.0.0/0.*	ACCEPT	↑ ↓	 
LAN-WAN-NTP-Accept	IPv4 and IPv6	UDP	lan:0.0.0.0/0.*	wan:0.0.0.0/0:123	ACCEPT	↑ ↓	 
LAN-WAN-DNS-Accept	IPv4 and IPv6	TCP+UDP	lan:0.0.0.0/0.*	wan:0.0.0.0/0:53	ACCEPT	↑ ↓	 
LAN-WAN-HTTP-Accept	IPv4 and IPv6	TCP	lan:0.0.0.0/0.*	wan:0.0.0.0/0:80	ACCEPT	↑ ↓	 
LAN-WAN-HTTPS-Accept	IPv4 and IPv6	TCP	lan:0.0.0.0/0.*	wan:0.0.0.0/0:443	ACCEPT	↑ ↓	 
LAN-WAN-FTP-Accept	IPv4 and IPv6	TCP	lan:0.0.0.0/0.*	wan:0.0.0.0/0:21	ACCEPT	↑ ↓	 

 Add

 Reset  Save  Save & Apply

Eingebaute Firewall Regeln (2)

◆ Datei: /etc/config/firewall (Beispiele)

◆ Regel für stateless DHCPv6

```
config 'rule'  
  option 'src'          'wan'  
  option 'proto'        'udp'  
  option 'src_ip'       'fe80::/10'  
  option 'src_port'     '547'  
  option 'dest_ip'      'fe80::/10'  
  option 'dest_port'    '546'  
  option 'family'       'ipv6'  
  option 'target'       'ACCEPT'  
  option 'name'         'Allow-DHCPv6'  
  option '_name'        'WAN-DEVICE-DHCPv6-Reply-Accept'
```

◆ Regel für ausgehendes HTTP

```
config 'rule'  
  option 'src'          'lan'  
  option 'dest'         'wan'  
  option 'proto'        'tcp'  
  option 'dest_port'    '80'  
  option 'target'       'ACCEPT'  
  option '_name'        'LAN-WAN-HTTP-Accept'
```

Fehlersuche

Fehlersuche

- ♦ **syslog**
- ♦ **tcpdump**
- ♦ **iptables / ip6tables**

Weitere Informationen

IPv6 & Linux bezogene Information

- ♦ **OpenWRT IPv6 HOWTO**
 - ♦ <http://wiki.openwrt.org/doc/howto/ipv6>
- ♦ **SixXS/ aiccu/ OpenWRT**
 - ♦ https://www.sixxs.net/wiki/Aiccu/Installing_on_OpenWRT

Kontakt-Information

peter@deepspace6.net

<http://www.deepspace6.net/>



pb@bieringer.de

<http://www.bieringer.de/pb/>

<http://www.bieringer.de/linux/IPv6/>

<http://mirrors.bieringer.de/>

Vielen Dank für die Teilnahme!

Fragen & Antworten

Tutorial mit Notizen ist als PDF per E-Mail bzw. über Veranstalter erhältlich!

Dankeschön an

Jürgen Seeger, iX & Johannes Endres, c't (Einladung)