Debian as advanced home router

jens::link

Setup

- Telekom FTTH
- Telekom PON
- APU / PC-Engines (EOL :-( )
- Also for DSL

Getting Addresses (I)

- pppoe (Point to Point Protocol over Ethernet)
- RFC2516
- Install *pppoe* and *pppoeconf* packages
- Run *pppoeconf*, answer questions

Getting Addresses (II)

- IPv4 address: via PPPoE
- 1 IPv6 address: via PPPoE / autoconfiguration
- Prefix: via dhcp-pd

dhcp-pd: distributing IPv6 prefixes (I)

- I'm using wide-dhcp:

```
interface ppp0 {
        send ia-pd 0;
};

id-assoc pd 0 {
        prefix-interface enp2s0 {
                sla-len 8;
                sla-id 1;
        };
};
```

Router Advertisement distributing IPv6 prefixes (I)

- radvd

```
interface enp2s0
{
    AdvLinkMTU 1492;
        AdvSendAdvert on;
        prefix ::/64
        {
                AdvOnLink on;
                AdvAutonomous on;
                AdvRouterAddr on;
        };

        RDNSS 2003:a:461:3b01:20d:b9ff:fe4f:ac6d
        {
        };
    DNSSL example.com
    {
    };
};
```

jens::link

setting up routing

```
cat /etc/sysctl.d/01-ipv6-forward.conf
01-ipv6-forward.conf:net.ipv6.conf.all.forwarding = 1
01-ipv6-forward.conf:net.ipv6.conf.ppp0.accept_ra = 2
```

A router MUST NOT accept RAs. On Linux the “2” overrules this behavior.

Firewalling IPv4 / IPv6 / NAT

- There are many good tutorials out there
- Recommendations for Filtering ICMPv6 Messages in Firewalls

Setting up DHCPv4 (Kea)

```
"subnet4": [
        {
            "subnet": "192.168.1.0/24",
            "interface": "enp0s8",
            "pools": [
                {
                    "pool": "192.168.1.100-192.168.1.199"
                }
            ],

            "option-data": [
                {
                    "name": "routers",
                    "data": "192.168.1.1"
                },
                {
                    "name": "domain-name-servers",
                    "data": "192.0.2.1"
                }
            ],
```

jens::link

DHCPv6

- I'm not using DHCPv6
- Flags in the RA are only a hint that DHCPv6 is available client may try without the flags

Setting up a DNS Resolver

- I'm using unbound

```
server:
    verbosity: 1
    statistics-interval: 1
    extended-statistics: yes
    num-threads: 1
    interface: 192.0.2.1
    interface: ::1
    interface: 127.0.0.1
    interface: 3fff:1000::1
    port: 53
    do-ip4: yes
    do-ip6: yes
    do-udp: yes
    do-tcp: yes
    do-daemonize: yes
```

Setting up a DNS resolver

```
access-control: 0.0.0.0/0 refuse
access-control: 127.0.0.0/8 allow
access-control: ::1 allow
access-control: 192.0.2.0/24 allow
access-control: 3fff:1000::/56 allow
directory: "/etc/unbound"
include: "/etc/unbound/unbound.conf.d/ad-blacklist.conf"
logfile: /var/log/unbound.log
log-queries: no
log-time-ascii: no
pidfile: "/var/run/unbound.pid"
```

Blacklist

https://raw.githubusercontent.com/StevenBlack/hosts/master/hosts

Going IPv6 only - NAT64

- I'm using tyaga
- Also take a look at https://www.jool.mx/en/run-nat64.html

```
tun-device nat64
ipv4-addr 198.51.100.1
ipv6-addr 2001:db8::1
prefix 64:ff9b::/96
dynamic-pool 198.51.100.0/24
data-dir /var/spool/tayga
```

Going IPv6 only - DNS64 (I)

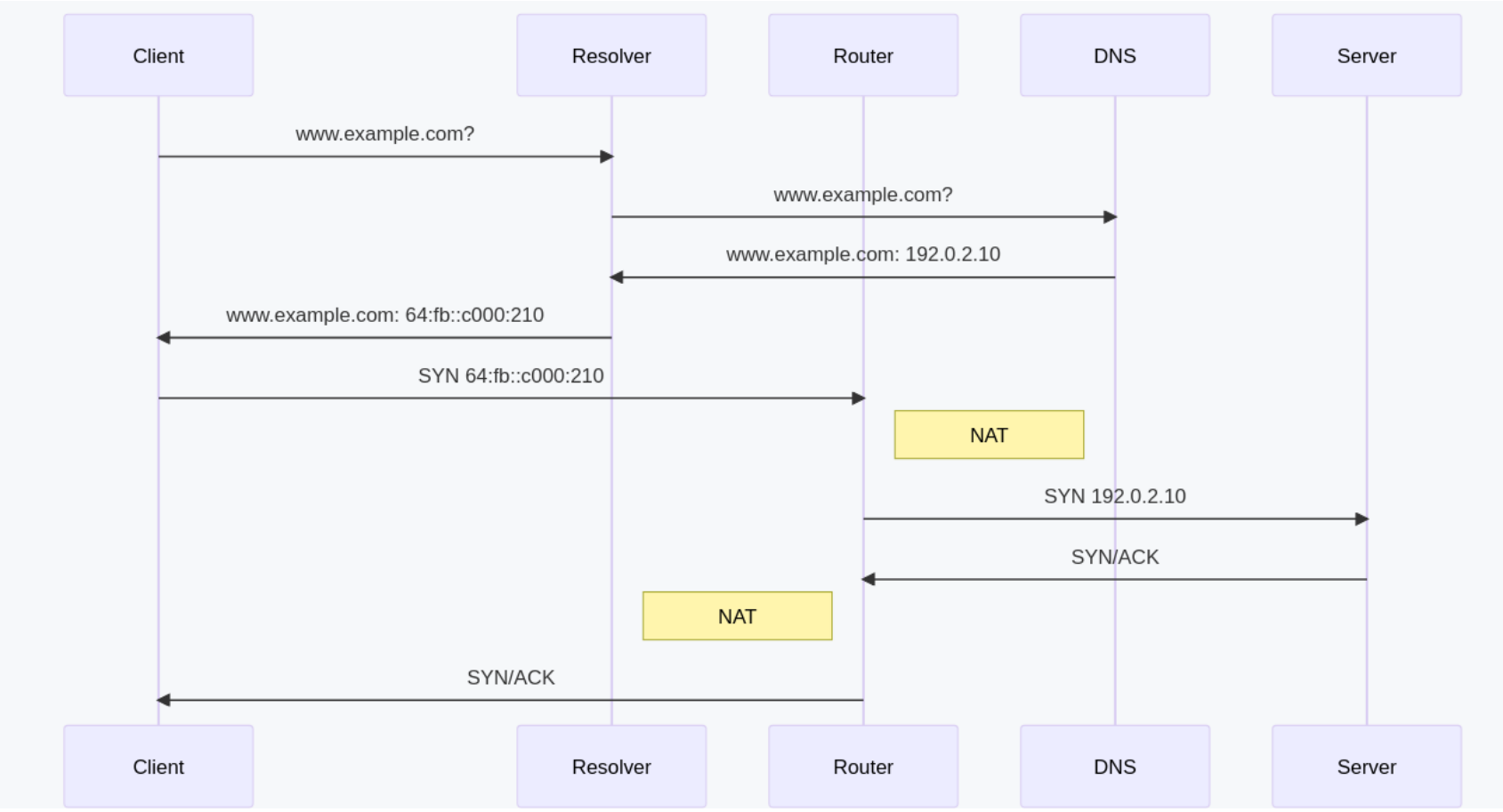

Figure 1: DNS64

jens::link

Going IPv6 only - DNS64 (II)

- I'm using a seconed Unbound instance

```
module-config: "dns64"
dns64-prefix: 64:FF9B::/96
```

Going IPv6 only - 464XLAT

- For Linux: https://github.com/toreanderson/clatd
- Windows 11 will ship with this in late 2024

Going back: Implementing IPv6 mostly

- Add the following to your IPv4 DHCP config:

```
"subnet4": {
    "option-data": [
        "name": "v6-only-preferred",
        "data": "3600" ]
        }
```

The End

- Questions?