Using a Juniper SRX 300 with a KPN fiberglas (glasvezel) internet connection

1. Prelude

A lot of folks in the Netherlands who are technically inclined, want to replace their ISP supplied modem with something more…. well, ***more*** basically.

As I am a Juniper and Cisco contractor / instructor, I decided a few years ago to get rid of the Experiabox supplied by KPN and replace it with a Juniper SRX. I love the SRX boxes: they are not too expensive, are full of tricks (and sometimes pitfalls..) and give me (almost) every option in the book.

So here goes..

2. The VLANs and TRUNK configuration

Internet comes in on VLAN 6 and voice on VLAN 7, via a trunk, as this website will tell you: http://netwerkje.com/eigen-router

Now unfortunately KPN (wisely) will not allow you to see the SIP / Voice credentials. So as far as I am aware, I cannot completely drop the $%^&*() modem – I will still need it for terminating the VOICE VLAN 7.

Since the SRX is both a switch as well as a Firewall, the first thing I did is to create the necessary VLANs: (I do not use IPtv)

```
SRX300# show vlans
vlan-internet {
    vlan-id 6;
    l3-interface irb.6;
}
vlan-voip {
    vlan-id 7;
    l3-interface irb.7;
```

The interface towards KPN is configured as a Trunk:

```
SRX300# show interfaces
ge-0/0/0 {
    description "Trunk towards KPN Internet";
    mtu 1518;
    unit 0 {
        family ethernet-switching {
            interface-mode trunk;
            vlan {
                members [ vlan-internet vlan-voip ];
```

One interface is used to switch the voice vlan to the Experiabox modem for voice:

```
ge-0/0/1 {
    description "VOIP VLAN access port";
    unit 0 {
        family ethernet-switching {
            interface-mode trunk;
            vlan {
```

```
            members vlan-voip;
```

VLAN 6 (internet) requires a PPPoe interface. SRXs do NOT SUPPORT PPPOE ON A VLAN INTERFACE. (and yes that sucks)
They do on a VLAN-Tagging interface but that is a router-on-a-stick, which is not what I am after.

SO.. how do I get this done if I cannot run PPPoe on a VLAN interface?.. well this part is a bit filthy: I could of course simply take a switch and split off VLAN 6 as an access port and connect it to the SRX. Then that access port could be used by PPPOE. But it requires an extra switch,- which I have but I want to keep my number of cables (and devices) to a bare minimum. (easier for troubleshooting)

So what I did was.. interface 3 became an access port in VLAN 6:

```
ge-0/0/3 {
    description "Access port in vlan-internet to ge-0/0/4 to allow PPPoe
VLAN";
    unit 0 {
        family ethernet-switching {
            interface-mode access;
            vlan {
                members vlan-internet;
```

3. The PPPoe configuration

This interface 3 is connected directly to the next interface (loop!...) 4. This interface is now the basis for the PPPoe interface..

```
ge-0/0/4 {
    unit 0 {
        description "IF with Internet IP via PPPoE";
        encapsulation ppp-over-ether;
```

And this is what the PPPoe interface definition looks like:

```
pp0 {
    inactive: traceoptions {
        flag all;
    }
    unit 0 {
        ppp-options {
            pap {
                local-name "**********************";
                local-password ********************"; ## SECRET-DATA
                passive;
            }
        }
        pppoe-options {
            underlying-interface ge-0/0/4.0;
            auto-reconnect 3;
            client;
        }
        family inet {
```

```
            mtu 1492;
            negotiate-address;
```

Now.. once you add the PPPoe interface to your "untrust zone" and you get your PPPoe interface up.. say hellalujah!

```
# run show interfaces pp0 terse
Interface               Admin Link Proto    Local                 Remote
pp0                     up    up
pp0.0                   up    up   inet     84.87.114.31 --> 195.190.228.34
```

Add a default route and try a ping:

```
set routing-options static route 0.0.0.0/0 next-hop pp0.0
```

```
SRX300> ping inet google.com
PING google.com (172.217.19.206): 56 data bytes
64 bytes from 172.217.19.206: icmp_seq=0 ttl=119 time=10.873 ms
```

4. And now the fun begins..

Once you have gotten this far, the rest is a lot of work but pretty standard:
-Configure your security zones and add the internal interfaces.
-Configure the DHCP server(s).
-Configure your Source NAT configuration.
-Configure security policies for destination nat etc. (port – forwarding)
-Configure Internet screens if you dare..

5. Things that are NOT working.. OR ARE THEY?!

The configuration above has been running for ages. Initially on my SRX 210, and for about 3 years on my SRX 300,- which I love. And the performance is good as well. (NAT works without a hitch for the full 200Mbps)

BUT.. there was one thing that I COULD ***NOT*** get to work:
-IPv6 over PPPoe should work on the KPN network. No matter what settings I tried, the PPPoe client would not receive a SLAAC address for PD from KPN. And I tried this with multiple Junos versions by the way.

My configuration looked something like this:

```
family inet6 {
        dhcpv6-client {
            client-type stateful;
            client-ia-type ia-na;
            client-ia-type ia-pd;
            client-identifier duid-type duid-ll;
            req-option dns-server;
            retransmission-attempt 9;
            update-server;
        }
        mtu 1492;
        negotiate-address;
```

The problem remaind very persistent. Tracefiles of PPPoe.. reboots, restarts.. I have tried them all. And it should be possible.. so if some guru (read: fellow nerd) in the Netherlands has more success with this, I would be most obliged if you drop me a line.

I tried the Juniper suggested settings like this one:
https://kb.juniper.net/InfoCenter/index?page=content&id=KB30956&cat=SRX_650&actp=LIST

There is conflicting documentation that states that IPv6 is not supported on a PPPoe interface either on Junos or on the SRX specifically. If that is true and the reason for my dismay, then that is very disappointing.

This forum: https://forums.juniper.net/t5/SRX-Services-Gateway/SRX100-IPv6-PPPoE-No-DHCPv6-available/td-p/135661

States:
"This is Srinath from SRX TAC. Just wanted to let you know that pp0 interface is not supported as a DHCPv6 client. This is confirmed for all active releases currently available (11.n till 15.1X release train) as such there seem to be no plans to support this feature."

Other documentation states complete configurations of PPPoe and IPv6 client functionality:
https://kb.juniper.net/InfoCenter/index?page=content&id=KB30824&cat=SRX_550&actp=LIST

The problem remaind:

```
SRX300> show dhcpv6 client binding detail

Client Interface/Id: pp0.0
     Hardware Address:              **:**:**:**:**:**
     State:                         INIT(DHCPV6_CLIENT_STATE_INIT)
     ClientType:                    STATEFUL
     Bind Type:                     IA_NA IA_PD
     Preferred prefix length        0
     Sub prefix length              0
     Client DUID:                   LL0x**-**:**:**:**:**:**
     Rapid Commit:                  Off
     Server Identifier:             ::/0
     Update Server                  Yes
     Client IP Address:             ::/0
     Client IP Prefix:              ::/0
```

6. UPDATE on feb. the 3rd 2021

Today I got a very kind email from Bill Gertz, who not only expressed his gratitude as it helped him to get his "KPN Glasvezel" connection going on the SRX, BUT.. he got native IPv6 working on the SRX as well!

Using a Juniper SRX 300 with a KPN fiberglas (glasvezel) internet connection

I am much indebted to him as his remarks helped me to get IPv6 working as well. So here are the missing pieces that got it to work on my SRX:

Pp0 configuration for IPv6:

```
   family inet6 {
        dhcpv6-client {
            client-type stateful;
            client-ia-type ia-pd;
            client-identifier duid-type duid-ll;
            req-option dns-server;
            retransmission-attempt 9;
            inactive: update-router-advertisement {
                interface irb.3 {
                    max-advertisement-interval 20;
                }
            }
            update-server;
        }
        mtu 1492;
```

The main thing was to drop the rapid-command and then something else needed to be done.. see below.

After the changes to the configuration above, the DHCP dialogue would still be stuck in either “INITIALIZING” or “SELECTIN**G**”:

```
SRX300# run show dhcpv6 client binding detail

Client Interface/Id: pp0.0
     Hardware Address:             **:**:**:**:**:**
     State:                        SELECTING(DHCPV6_CLIENT_STATE_SELECTING)
     ClientType:                   STATEFUL
     Bind Type:                    IA_PD
     Preferred prefix length       0
     Sub prefix length             0
     Client DUID:                  LL0x29-**:**:**:**:**
     Rapid Commit:                 Off
     Server Identifier:            ::/0
     Update Server                 Yes
     Client IP Prefix:             ::/0
```

Then the next step was.. to clear the Pppoe sessions..

```
SRX300# run clear pppoe sessions pp0.0
```

That did the trick!

```
SRX300> show dhcpv6 client binding detail

Client Interface/Id: pp0.0
     Hardware Address:             **:**:**:**:**:**
     State:                        BOUND(DHCPV6_CLIENT_STATE_BOUND)
     ClientType:                   STATEFUL
     Lease Expires:                2021-02-06 20:09:57 CET
     Lease Expires in:             259171 seconds
     Lease Start:                  2021-02-03 20:09:57 CET
```

```
Bind Type:                    IA_PD
Preferred prefix length       0
Sub prefix length             0
Client DUID:                  LL0x29-**:**:**:**:**
Rapid Commit:                 Off
Server Identifier:            fe80::da49:bff:feb7:2e21
Update Server                 Yes
Client IP Prefix:             ****:****:****::/48
```

Next question is.. since your WAN interface does NOT get an IPV6 address assigned.. which IPv6 addresses can I use?

The "`Client IP Prefix`" is the /48 prefix that you can subnetwork to your heart's content. So in my case I went mad and created two SVIs within the same /48 prefix.

Small bits that I should not forget to mention are:
The default-gateway for IPv6 should point to your ISP:

```
set routing-options rib inet6.0 static route ::/0 next-hop pp0.0
```

Of course the IPv6 Routing-engine should be enabled:

```
set security forwarding-options family inet6 mode flow-based
```

And the DHCPv6 service should be allowed on the untrust zone and the interface pp0.0 be part of that zone:

```
set security zones security-zone untrust interfaces pp0.0
set security zones security-zone untrust host-inbound-traffic system-services dhcpv6
```

This has been quite an uphill struggle.. but in the end.. JUNIPER RULES.

7. The only quest left..

Then the other thing that REALLY annoys me on the SRX: getting a remote access IPsec VPN tunnel to work towards my OsX Apple laptop ***WITHOUT*** using commercial clients like Pulse[1] Secure (why Juniper sold of that successful product line is beyond me) or NCP.

I tried IPsecuritas, shrew, the build in OsX IPsec clients; no joy.
So for the VPN I had to resort to Linux and the ***free***, opensource alternatives OpenVPN (brilliant) and Strongswan. (easy) Both perform excellent but require again more boxes and complexity and port-forwarding, while I have an enterprise grade firewall at my disposal.

I find it questionable why enterprise vendors (Cisco / Juniper, many others) dare to ask money for something mundane as VPN connections and clients after you have already bought their solutions, while there are so many free alternatives available.

And apparently I am not the only one..

[1] See other articles on my website on how to setup an IPsec remote access VPN with Pulse secure and the SRX

Using a Juniper SRX 300 with a KPN fiberglas (glasvezel) internet connection

Juniper's lack of remote access VPN support in this is one of a number of reasons why customers (like the Dutch Police department) are turning their backs on the Juniper SRX and are moving towards Fortigate. (sigh..)

I hope this has helped a few diehard Juniper lovers like me.