IPv6 Tunnelbroker (Hurricane Electric)

Diese Anleitung soll die Einrichtung eines 6to4 IPv6 Tunnels beschreiben. Bitte die Anleitung nicht einfach per Copy&Paste durcharbeiten, sondern auch verstehen. Meine persönlichen Angaben zum Tunnel oder Zugangsdaten wurden anonymisiert oder geschwärzt.

Mit dem IPv6 Tunnelbroker bietet Hurricane Electric (HE) einen kostenlosen 6to4 Tunnelservice an (ähnlich wie Sixxs, nur ist HE nicht so assig und unfreundlich). Man bekommt direkt ein /64er Netz zugewiesen und verfügt damit über 18446744073709551616 IP-Adressen. Das sollte eine Weile ausreichen. Man kann sich auch ein /48er Netz geben lassen. In ein /48 passen nochmal 65536 /64er Netze. Das entspricht dann 1208925819614629174706176 IPv6-Adressen.

Um nun den Tunnelbroker Service mit Ubiquiti EdgeMAX Routern verwenden zu können sind ein paar vorbereitende Schritte notwendig. Verfügt man über eine statische IP für den Internetzugang, kann der DynDNS-Teil weg gelassen werden. Die Anleitung geht im Folgenden davon aus, dass man seine WAN-IP dynamisch zugeteilt bekommt.

1. Anmeldung bei Tunnelbroker
2. einen IPv6 Tunnel registrieren
3. Anmeldung bei DNS-O-MATIC. Dieser kostenlose Service kann verschiedenste andere Services über eine neu zugeteilte WAN-IP informieren. Ich nutze das z.B. mit afraid.org (dynDNS Provider) und um die clientseitige Tunnel-IP bei HE zu setzen, da sonst der Tunnel nicht aufgebaut werden kann

DNS-O-MATIC

Beginnen wir mit der Konfiguration von DNS-O-MATIC. Auf deren Webseite habe ich die beiden Services afraid.org und Tunnelbroker angelegt.

Bei afraid.org kann man sich eine Subdomain unter verschiedensten Domains aussuchen und diese bei einer Änderung der WAN-IP durch seinen Router oder andere Mechanismen automatisch mit der neuen IP updaten lassen.

Um das durch DNS-O-MATIC erledigen zu lassen, besorgt man sich auf der afraid-Seite http://freedns.afraid.org/dynamic/ seinen Update-Key. Dieser versteckt sich bei der registrierten Subdomain hinter dem „Direct URL“ Link. Einfach den String nach „http://freedns.afraid.org/dynamic/update.php?“ rauskopieren und in das Key-Feld bei DNS-O-MATIC eintragen und speichern.

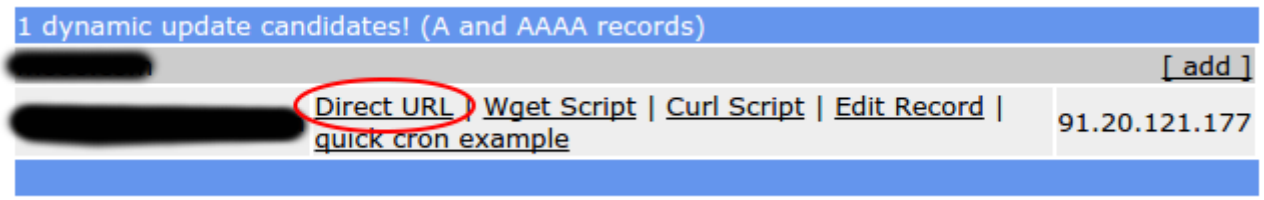

Abb.1

Um die IP bei Tunnelbroker auch updaten zu können braucht man folgende Infos von deren Seite:

- Username (nicht die lange User-ID, die im Inhaltsteil nach dem Login angezeigt wird)
- Passwort ist der Update Key auf der Detailseite des Tunnels (Advanced), alternativ das Tunnelbroker Passwort, wenn man keinen Update Key hat
- den DNS-Namen des Tunnel. Dieser wird z.B. auf der Übersichtsseite angezeigt und hat folgendes Format: <user>-<index>.tunnel.<tunnel-server>.<datacenter>.ipv6.he.net

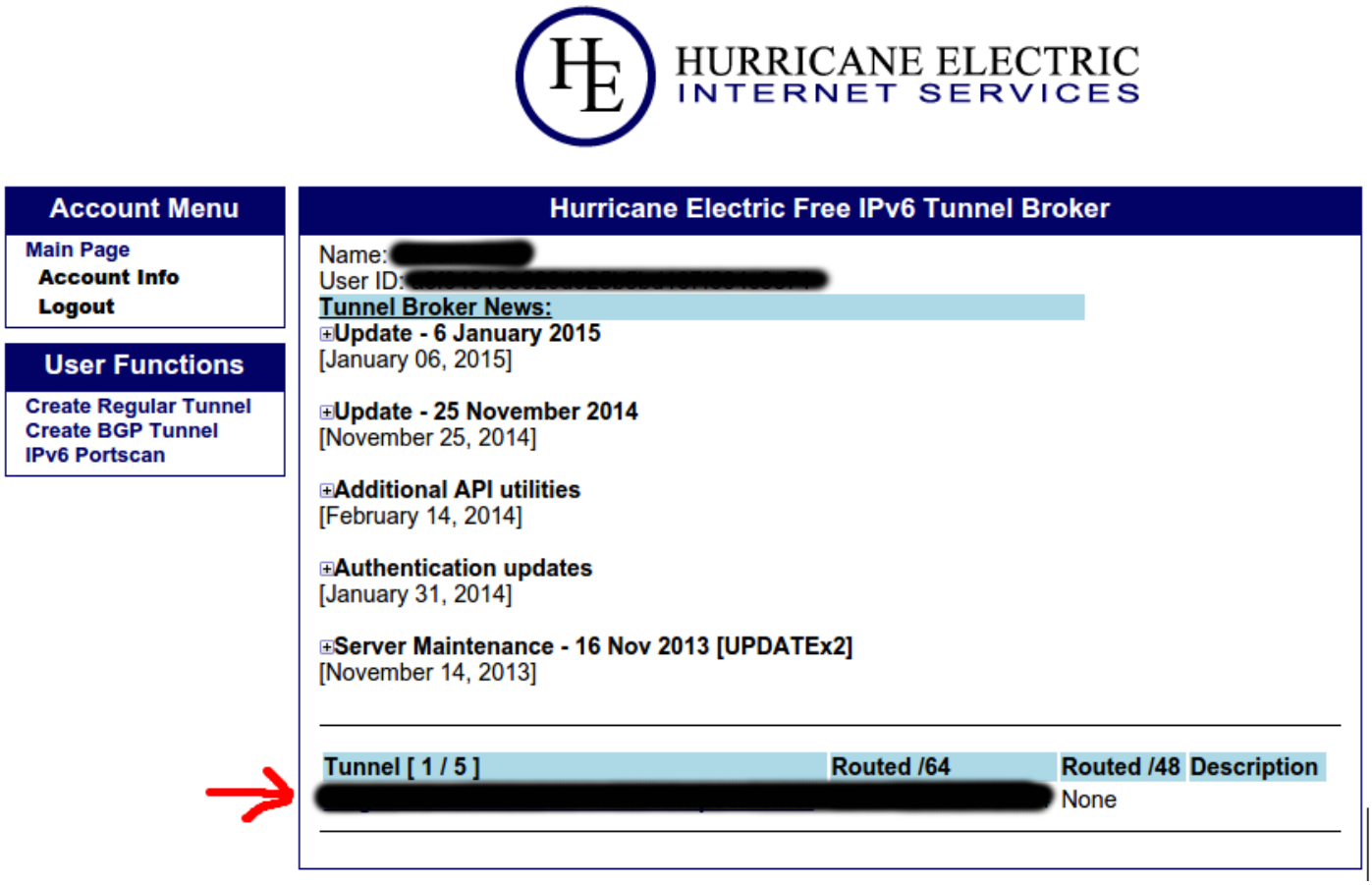

Abb.2

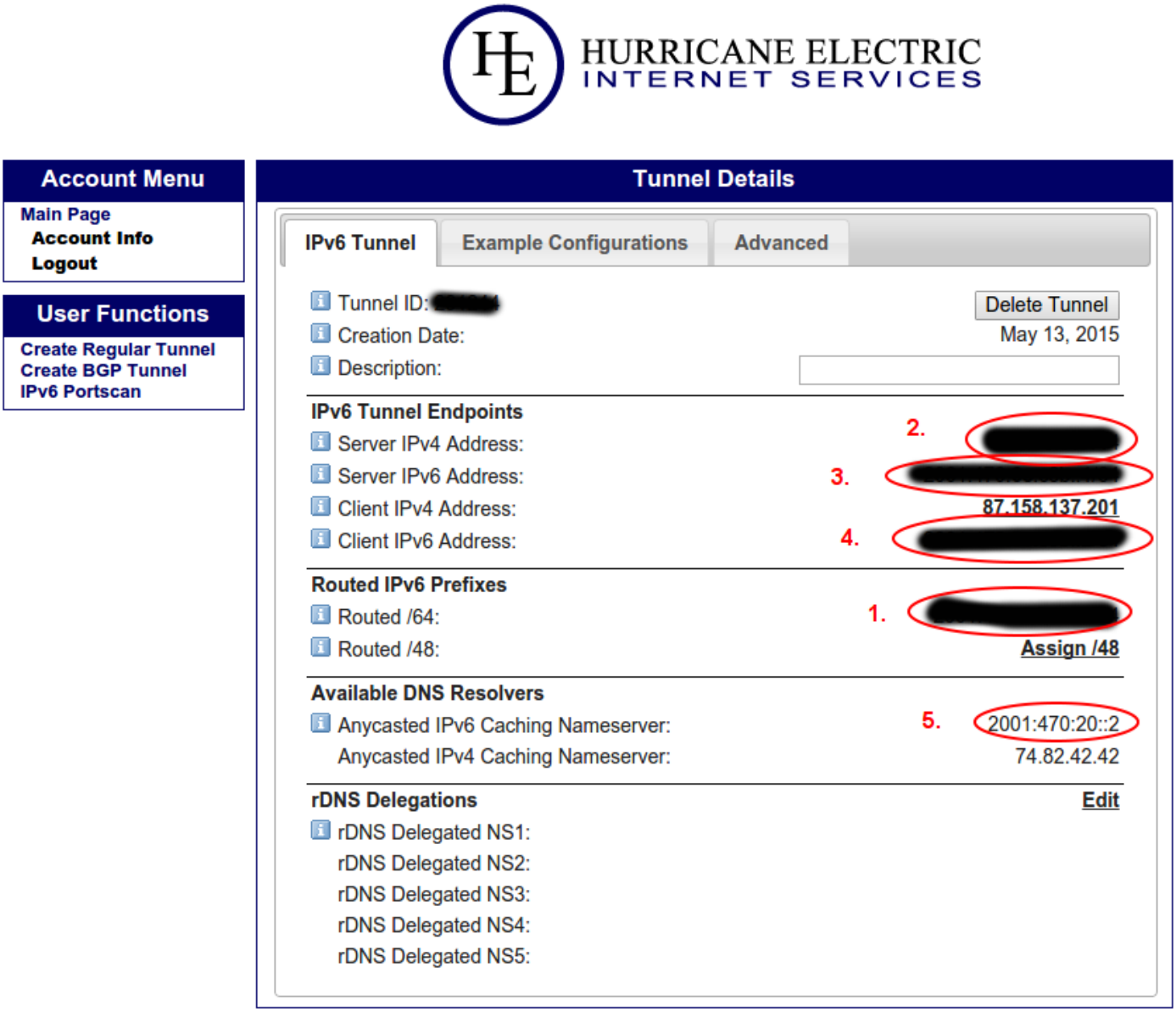

Abb.3

Damit wäre der Dyndns-Service vorbereitet und kann auf dem Router konfiguriert werden (pppoe0 ist mein WAN-Interface):

```
admin@gate:~$ configure

set service dns dynamic interface pppoe0 service dyndns host-name all.dnsomatic.com
set service dns dynamic interface pppoe0 service dyndns login <dns-o-matic login>
set service dns dynamic interface pppoe0 service dyndns password <dns-o-matic passwort>
set service dns dynamic interface pppoe0 service dyndns protocol dyndns2
set service dns dynamic interface pppoe0 service dyndns server updates.dnsomatic.com

commit
save
exit
```

Will man gleich testen, ob das klappt, erzwingt man am einfachsten einen Reconnect:

```
admin@gate:~$ disconnect interface pppoe0
admin@gate:~$ connect interface pppoe0
```

Auf der DNS-O-MATIC-Seite sollten nun beide Services mit einem grünen Daumen-hoch markiert und die aktuelle IP hinterlegt sein.

Bevor der Tunnel konfiguriert wird, empfiehlt es sich eine passende Firewall zu konfigurieren. Mit LOCAL_TUN0 ist dabei ausgehender Datenverkehr (LAN ? WAN), TUN0_LOCAL eingehend zum Router, TUN0_IN eingehend ins lokale Netz (FORWARD) gemeint. Das kann dann z.B. so aussehen:

```
admin@gate:~$ configure

set firewall all-ping enable
set firewall broadcast-ping disable
set firewall ipv6-name LOCAL_TUN0 default-action accept
set firewall ipv6-name LOCAL_TUN0 description 'outgoing to IPv6 Tunnel'
set firewall ipv6-name TUN0_IN default-action drop
set firewall ipv6-name TUN0_IN description 'IPv6 Tunnel to local net'
set firewall ipv6-name TUN0_IN enable-default-log
set firewall ipv6-name TUN0_IN rule 1 action accept
set firewall ipv6-name TUN0_IN rule 1 description 'Must be allowed or MTU discovery will break'
set firewall ipv6-name TUN0_IN rule 1 icmpv6 type packet-too-big
set firewall ipv6-name TUN0_IN rule 1 protocol icmpv6
set firewall ipv6-name TUN0_IN rule 2 action accept
set firewall ipv6-name TUN0_IN rule 2 description 'Allow ICMP echo reply'
set firewall ipv6-name TUN0_IN rule 2 icmpv6 type pong
set firewall ipv6-name TUN0_IN rule 2 limit burst 1
set firewall ipv6-name TUN0_IN rule 2 limit rate 50/minute
set firewall ipv6-name TUN0_IN rule 2 protocol icmpv6
set firewall ipv6-name TUN0_IN rule 3 action accept
set firewall ipv6-name TUN0_IN rule 3 description 'May cause fragmentation issues otherwise'
set firewall ipv6-name TUN0_IN rule 3 icmpv6 type time-exceeded
set firewall ipv6-name TUN0_IN rule 3 protocol icmpv6
set firewall ipv6-name TUN0_IN rule 4 action accept
set firewall ipv6-name TUN0_IN rule 4 description 'Allow established/related'
set firewall ipv6-name TUN0_IN rule 4 protocol all
set firewall ipv6-name TUN0_IN rule 4 state established enable
set firewall ipv6-name TUN0_IN rule 4 state invalid disable
set firewall ipv6-name TUN0_IN rule 4 state new disable
set firewall ipv6-name TUN0_IN rule 4 state related enable
set firewall ipv6-name TUN0_IN rule 5 action drop
set firewall ipv6-name TUN0_IN rule 5 description 'Drop invalid state'
set firewall ipv6-name TUN0_IN rule 5 log disable
set firewall ipv6-name TUN0_IN rule 5 protocol all
set firewall ipv6-name TUN0_IN rule 5 state established disable
set firewall ipv6-name TUN0_IN rule 5 state invalid enable
set firewall ipv6-name TUN0_IN rule 5 state new disable
set firewall ipv6-name TUN0_IN rule 5 state related disable
set firewall ipv6-name TUN0_LOCAL default-action drop
set firewall ipv6-name TUN0_LOCAL description 'IPv6 Tunnel to EdgeRouter'
set firewall ipv6-name TUN0_LOCAL enable-default-log
set firewall ipv6-name TUN0_LOCAL rule 1 action accept
set firewall ipv6-name TUN0_LOCAL rule 1 description 'Must be allowed or MTU discovery will brea
set firewall ipv6-name TUN0_LOCAL rule 1 icmpv6 type packet-too-big
set firewall ipv6-name TUN0_LOCAL rule 1 protocol icmpv6
set firewall ipv6-name TUN0_LOCAL rule 2 action accept
set firewall ipv6-name TUN0_LOCAL rule 2 description 'Allow ICMP echo reply'
set firewall ipv6-name TUN0_LOCAL rule 2 icmpv6 type pong
set firewall ipv6-name TUN0_LOCAL rule 2 limit burst 1
set firewall ipv6-name TUN0_LOCAL rule 2 limit rate 50/minute
set firewall ipv6-name TUN0_LOCAL rule 2 protocol icmpv6
set firewall ipv6-name TUN0_LOCAL rule 3 action accept
set firewall ipv6-name TUN0_LOCAL rule 3 description 'May cause fragmentation issues otherwise'
set firewall ipv6-name TUN0_LOCAL rule 3 icmpv6 type time-exceeded
set firewall ipv6-name TUN0_LOCAL rule 3 protocol icmpv6
set firewall ipv6-name TUN0_LOCAL rule 4 action accept
set firewall ipv6-name TUN0_LOCAL rule 4 description 'Allow established/related'
set firewall ipv6-name TUN0_LOCAL rule 4 protocol all
set firewall ipv6-name TUN0_LOCAL rule 4 state established enable
set firewall ipv6-name TUN0_LOCAL rule 4 state invalid disable
set firewall ipv6-name TUN0_LOCAL rule 4 state new disable
set firewall ipv6-name TUN0_LOCAL rule 4 state related enable
set firewall ipv6-name TUN0_LOCAL rule 5 action drop
set firewall ipv6-name TUN0_LOCAL rule 5 description 'Drop invalid state'
set firewall ipv6-name TUN0_LOCAL rule 5 log disable
set firewall ipv6-name TUN0_LOCAL rule 5 protocol all
set firewall ipv6-name TUN0_LOCAL rule 5 state established disable
set firewall ipv6-name TUN0_LOCAL rule 5 state invalid enable
set firewall ipv6-name TUN0_LOCAL rule 5 state new disable
```

```
set firewall ipv6-name TUN0_LOCAL rule 5 state related disable
set firewall ipv6-receive-redirects disable
set firewall ipv6-src-route disable
set firewall ip-src-route disable
set firewall log-martians enable
set firewall receive-redirects disable
set firewall send-redirects enable
set firewall source-validation disable
set firewall syn-cookies enable

commit
save
exit
```

Für die Konfiguration des Tunnels werden noch folgende Daten von der Tunnelbroker Detailseite benötigt. HE gibt auch hier ein komplettes /64er als Transfernetz heraus:

- Client IPv6 Address (endet auf ::2/64, Abb.4.4)
- Server IPv4 Address (Abb.4.2)
- Routed IPv6 Prefixes (Abb.4.1)
- die eigene interne LAN-IP

Achtung: Die IPv6 Tunnel Endpunkte und der geroutete IPv6-Prefix sind unterschiedlich! Auf der Tunnelbroker-Seite sind diese deswegen auch dick hervorgehoben. Das muss bei der weiteren Konfiguration beachtet werden.

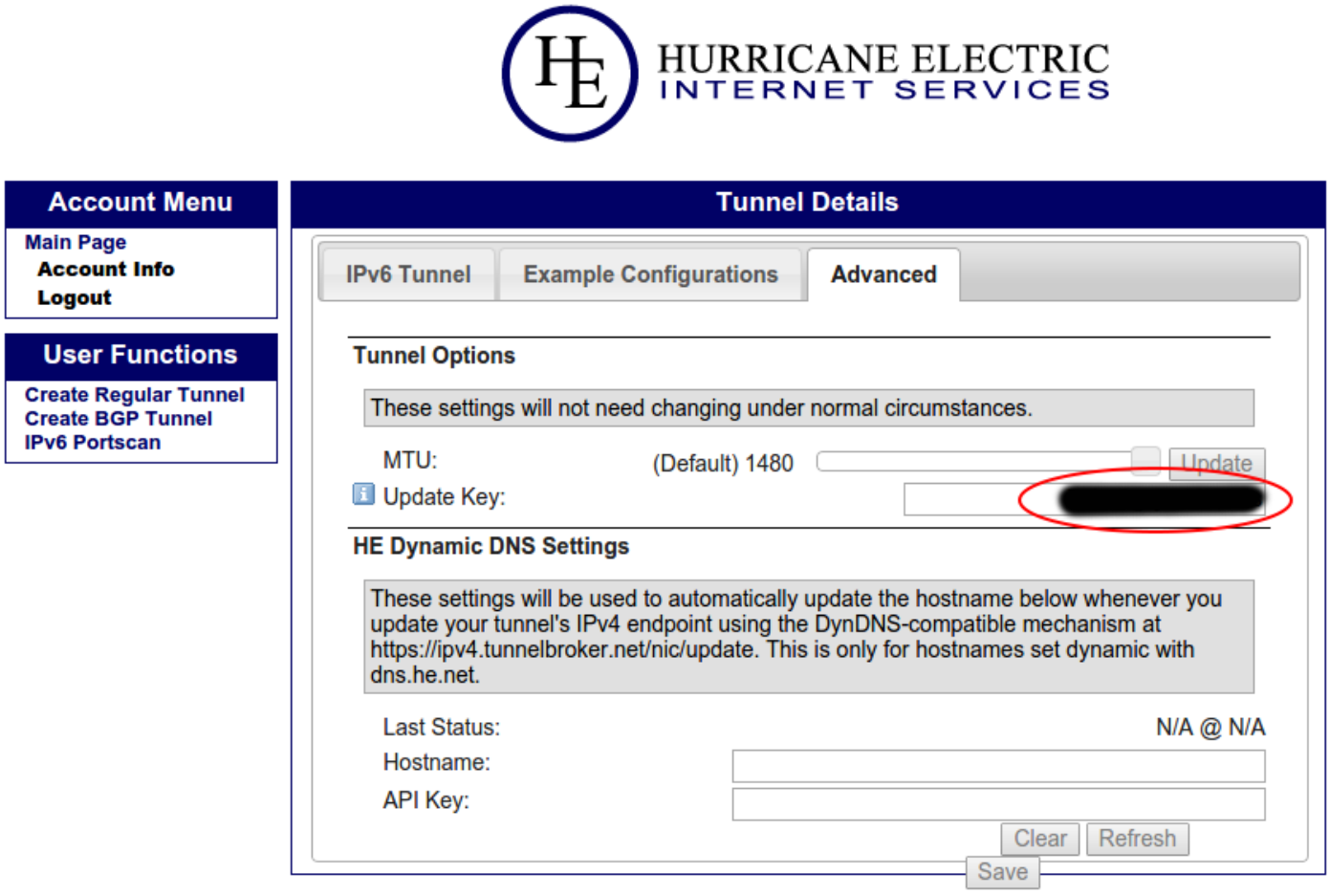

Abb.4

Die Konfiguration des Tunnels sieht dann so aus:

```
admin@gate:~$ configure
```

```
set interfaces tunnel tun0 address '<Client IPv6 Address>'
set interfaces tunnel tun0 description 'he.net IPv6 Tunnel'
set interfaces tunnel tun0 encapsulation sit
set interfaces tunnel tun0 firewall in ipv6-name TUN0_IN
set interfaces tunnel tun0 firewall local ipv6-name TUN0_LOCAL
set interfaces tunnel tun0 firewall out ipv6-name LOCAL_TUN0
set interfaces tunnel tun0 local-ip <interne LAN-IP>
set interfaces tunnel tun0 multicast disable
set interfaces tunnel tun0 remote-ip <Server IPv4 Address>
set interfaces tunnel tun0 ttl 255

commit
save
exit
```

Der Tunnel sollte nun schon aufgebaut sein. Die Firewall ist aktiviert.

```
admin@gate:~$ show interfaces tunnel tun0 brief
Codes: S - State, L - Link, u - Up, D - Down, A - Admin Down
Interface    IP Address                        S/L  Description
---------    ----------                        ---  -----------
tun0         <ipv6 network>/64                 u/u  he.net IPv6 Tunnel
```

„u/u“ bedeutet State und Link sind up, der Tunnel ist also funktional.

Damit das IPv6 Netz auch im LAN verwendbar wird, fehlen noch ein paar Dinge.

Erstmal wird eine IPv6-IP (die erste freie IP (::1 ist HE, ::2 deine Seite des Tunnels) aus deinem IPv6-Netz (::3) auf das LAN-Interface des Routers gelegt (bei mir ist das switch0). Danach werden noch die Default-Route für IPv6, DHCPv6 (soll nur für Nameserver, Searchdomain und NTP verwendet werden) und die Router-Adverts (d.h. die Clients konfigurieren sich ihre IPv6-Adresse anhand ihrer MAC-Adresse selbst) konfiguriert. Der Name-Server kommt von der Tunnelbroker Webseite (Abb.4.5).

```
admin@gate:~$ configure
set protocols static interface-route6 '::/0' next-hop-interface tun0

set service dhcpv6-server shared-network-name LAN1-IPv6 subnet '<ipv6 routed network>' domain-se
set service dhcpv6-server shared-network-name LAN1-IPv6 subnet '<ipv6 routed network>' name-serv
set service dhcpv6-server shared-network-name LAN1-IPv6 subnet '<ipv6 routed network>' sntp-serv

set interfaces switch switch0 address '<ipv6 routed network>::1/64'
set interfaces switch switch0 description LAN1
set interfaces switch switch0 dhcpv6-options parameters-only
set interfaces switch switch0 ipv6 dup-addr-detect-transmits 1
set interfaces switch switch0 ipv6 router-advert cur-hop-limit 64
set interfaces switch switch0 ipv6 router-advert default-preference high
set interfaces switch switch0 ipv6 router-advert link-mtu 1280
set interfaces switch switch0 ipv6 router-advert managed-flag false
set interfaces switch switch0 ipv6 router-advert max-interval 600
set interfaces switch switch0 ipv6 router-advert other-config-flag true
set interfaces switch switch0 ipv6 router-advert prefix '<ipv6 routed network>' autonomous-flag
set interfaces switch switch0 ipv6 router-advert prefix '<ipv6 routed network>' on-link-flag tru
set interfaces switch switch0 ipv6 router-advert prefix '<ipv6 routed network>' valid-lifetime 2
set interfaces switch switch0 ipv6 router-advert reachable-time 0
set interfaces switch switch0 ipv6 router-advert retrans-timer 0
set interfaces switch switch0 ipv6 router-advert send-advert true

commit
save
exit
```

Damit sollten sich nun die IPv6-fähigen Clients in eurem LAN bereits ihre Adresse geholt/erzeugt haben und über den Tunnel nach draußen gehen können.

Hier ein paar Möglichkeiten den IPv6-Verkehr zu beobachten / debuggen:

- Informationen zum Tunnel: show interfaces tunnel tun0 brief

- Packetdump: show interfaces tunnel tun0 capture
- Bytes, Packets und Fehlerraten zeigen: show interfaces tunnel detail
- Traceroute: traceroute6 www.heise.de
- Ping: ping6 www.heise.de

Revision #1
Created 2021-05-31 14:47:17 UTC by magenbrot
Updated 2021-05-31 14:49:29 UTC by magenbrot