Freifunk Troisdorf Gateway Doku

Release 0.1 beta

Freifunk-Troisdorf

Jan 14, 2018

Contents

In dieser Doku beschreiben wir unser Gluon/Linux Gateway Setup. Diese Daten stammen aus unserem Netz in Troisdorf, weshalb auch unsere IP Netze in den Config dateien zu finden sind.

Dieses Setup ist in mehreren Monaten entstanden, und kann dennoch noch einige Fehler enthalten. Wir versuchen unsere Gedankengänge hier so gut es geht zu umschreiben.

CHAPTER 1

Intro

1.1 Voraussetzungen

- voller Root Zugriff für alle Admins
- öffentliche IPv4 Adresse
- öffentliche IPv6 Adresse
- **voller Kernelzugriff**
  - Linux direkt installiert,
  - oder als KVM-Instanz (OpenVZ o.ä. nicht möglich)
- Hier genutzt: Debian 8

1.1.1 Betrieb und Zugang

Unsere Server werden momentan von 2 Personen Privat betriben. In unserem Setup ist immer nur 1 Server Aktiver Supernode, um unter anderem den Inter Gateway Traffic zu sparen. Dies funktioniert mit L2TP sehr gut, da die vorhandene Performance mit 1 Server ausreichend ist.

Wir installieren unsere Gateways per Ansible, was uns ein Identisches Setup per Server ermöglicht und uns neue Gateways innerhalb weniger Minuten ausrollen lässt. Die Ansible Config findet Ihr hier: [LINK EINFÜGEN]

1.1.2 Schema

Wie unser Netz aufgebaut ist seht ihr am einfachsten an dieser Darstellung:

1.1.3 Funktionen & dafür benötigte Software

Momentan kommen auf allen Gateways Debian 8 (jessie) zum Einsatz.

Für viele der Gate-Funktionen wird weitere Software benötigt, die alle aus den Debian Repositories nachinstalliert werden können.

See also:

- *Pakete*

Verbindung der Server und Nodes

Die Nodes bauen ihr Freifunk mit dem Mesh-Protokoll *B.A.T.M.A.N* selbständig auf.

Da das Netz aber noch nicht dicht genug ist, dass alle Nodes sich über ihre Funk-Interfaces erreichen können, helfen wir über eine VPN-Verbindung über das Internet nach, um einzelne Wolken zu überbrücken.

So wie über ihre Funk-Interfaces, sprechen die Nodes das *B.A.T.M.A.N* Protokoll auch über ihre VPN-Verbindungen.

Die Gateways sind die VPN Server für unsere Nodes. Die Nodes bauen alle einen L2TP Tunnel zu diesen auf.

Alle Gateways verbinden sich für das VPN auch vollständig untereinander. So entsteht eine Multi-Stern-Architektur. Alle Sternmittelpunkte sind untereinander voll vermascht.

Auf den Gateways wird hierzu **L2TP** sowie das Kernel Modul **batman_adv** benötigt.

See also:

- *Pakete*
- l2tp

DHCP für die Clients

Nodes, Clients und Gateways sind über ein Layer-2-Netz miteinander verbunden (*B.A.T.M.A.N*, s. o.).

Die Gateways halten auch als DHCP-Server für die Clients her.

Verfügbare IPv4-Ranges, aus denen der DHCP-Server vergeben darf, müssen innerhalb bzw. mit der Admin-Gruppe abgestimmt werden.

Hierfür wird **isc-dhcp-server** genutzt. Für das vorbereitende Ausrollen von IPv6 Adressen benötigen wir hier auch **radvd**.

See also:

- *DHCPd*
- radvd

Übergang ins restliche Internet

Die Verbindung ins Internet wird über den Freifunk Rheinland e.V. realisiert. Wir verbinden uns hierzu per **GRE** in das Backbone des FFRL und bekommen von hier auch Public IPv4 und IPv6 Adressen.

See also:

- *Pakete*
- *Netzwerk Interfaces*
- *Routing Tabellen*
- policyrouting
- *Internet-Exit*

Datenschutz auf dem Gateway

Unsere Gateways loggen keinen Traffic! Es werden lediglich Statistiken für die Bewertung der Auslastung unserer Gateways gespeichert.

Alles was existiert sind die zur Laufzeit benötigten Verbindungsdaten. DHCP-Leases, Batman Protokolldaten und die ARP-Tabelle.

Diese werden nur im Arbeitsspeicher vorgehalten, ist das Gateway aus (z.B. die Herren in Grün nehmen den Server mit), sind diese i.d.R. weg.

See also:

- logging

1.2 Netzplan

Freifunk Troisdorf ist ein IP Netz aus dem IPv4 Bereich `10.188.0.0/16`.

Wir haben unser IP Netz in Segmente eingeteilt um eine bessere Überischt zu haben.

1.2.1 IPv4

Wir haben für unserer Freifunk folgende Netze zugewiesen bekommen:

- Troisdorf - `10.188.0.0/16` = **188**

Datenpakete aus diesem Adressbereich werden innerhalb des Freifunks vermittelt, im großen weiten Internet aber nicht geroutet (Hintergrundinformationen dazu gibt es hier).

Unser großes `10.188.0.0/16` (mit 65536 Adressen) teilen wir uns ein wenig ein:

`10.188.0.0/16` wird nicht komplett genutzt, um in Zukunft noch was auf Halde zu haben. Wachsen ist immer einfacher als schrumpfen.

Netz	(bis)	Verwendung	verteilt durch	status
10.188.1.0/24	10.188.1.255	Services	fix	in Betrieb
10.188.2.0/24	10.188.2.255	Static IP Leases	Github/DHCP	Geblockt
10.188.100.1	10.188.103.255	Client DHCP-Range	troisdorf1	frei
10.188.104.1	10.188.107.255	Client DHCP-Range	troisodrf2	frei
10.188.108.1	10.188.111.255	Client DHCP-Range	troisdorf3	frei
10.188.112.1	10.188.115.255	Client DHCP-Range	troisdorf4	fre
10.188.116.1	10.188.119.255	Client DHCP-Range	troisodrf5	in Betrieb
10.188.120.1	10.188.124.255	Client DHCP-Range	troisdorf6	in Betrieb
10.188.125.1	10.188.128.255	Client DHCP-Range	troisdorf7	frei
10.188.255.0/24	10.188.255.255	Gateway IPs	fix	Geblockt

NEU:

Wir teilen das /16 in 8 /19 Netze ein.

Sub-Domäne 1 - Troisdorf

IPv4: 10.188.0.0/19

Netz	(bis)	Verwendung	verteilt durch	status
10.188.0.0/21	10.188.7.255	Netz Intern	fix	in Betrieb
10.188.8.0/21	10.188.15.255	Client DHCP-Range	•	in Betrieb
10.188.16.0/21	10.188.23.255	Client DHCP-Range	•	backup
10.188.24.0/21	10.188.31.255	frei	•	frei

IPv6: 2a03:2260:121:4000::/64 wird per Radvd announced

Sub-Domäne 2 - Troisdorf City IPv4: 10.188.32.0/19

Netz	(bis)	Verwendung	verteilt durch	status
10.188.32.0/18	10.188.39.255	Freie Verwenung	fix	in Betrieb
10.188.40.0/18	10.188.47.255	Client DHCP-Range	•	Geblockt
10.188.48.0/18	10.188.55.255	Client DHCP-Range	•	frei
10.188.56.0/18	10.188.63.255	Netz	•	frei

IPv6: 2a03:2260:121:5000::/64 wird per Radvd announced

Sub-Domäne 3 - Flüchtlinge IPv4: 10.188.64.0/19

Netz	(bis)	Verwendung	verteilt durch	status
10.188.64.0/18	10.188.71.255	Freie Verwendung	fix	frei
10.188.72.0/18	10.188.79.255	Client DHCP-Range	•	frei
10.188.80.0/18	10.188.87.255	Client DHCP-Range	•	frei
10.188.88.0/18	10.188.95.255	Client DHCP-Range	•	frei

IPv6: 2a03:2260:121:6000::/64 wird per Radvd announced

Subdomäne 4 - Events IPv4: “10.188.96.0/19

Netz	(bis)	Verwendung	verteilt durch	status
10.188.96.0/18	10.188.103.255	Freie Verwendung	fix	frei
10.188.104.0/18	10.188.111.255	Client DHCP-Range	•	frei
10.188.112.0/18	10.188.119.255	Client DHCP-Range	•	frei
10.188.120.0/18	10.188.127.255	Client DHCP-Range	•	frei

IPv6: 2a03:2260:121:7000::/64 wird per Radvd announced

1.2.2 IPv6

Wir nutzen das uns vom FFRL zugewiesene Public IPv6 Netz 2a03:2260:121::/48

IPv6 Subnetze haben immer eine Prefix-Länge von *64 Bit*. Durch das /48 Subnetz stehen uns also 2^16 = 65536 /64 IPv6 Subnetze zur Verfügung.

1.2.3 Interface Bezeichnung

Wir vergeben unsere Interface-Bezeichnungen einheitlich!

	eth0	Mesh - Bridge (Nodes)	B.A.T.M.A.N	Inter Gateway VPN	Exit VPN
		br-[SUB Name tdf, inn, flu]	bat[SUB NAME]	l2tp-*	gre-bb-*

1.2.4 Namenskonvention

Unsere Gateways sind durchnummeriert. Angefangen bei **troisdorf0** bis zu **troisdorf9**.

1.2.5 Next Node Adressen

Die Next Node Adressen sind dafür da, um sich im Fehler- oder Troubleshootingfall mit einem Freifunk Knoten zu verbinden.

Diese Adressen sind auf jedem Knoten gleich. Der Freifunker muss sich nur diese Adresse(n) merken und seine Netzwerkkarte für ein Subnetz konfigurieren, in dem diese Adresse(n) liegt um auf seinen Knoten zuzugreifen.

Wir nutzen dazu die jeweils niedrigsten Adressen

- **Troisdorf:**
  - IPv4: `10.188.0.1`
  - IPv6: `2a03:2260:121::1`

1.2.6 Gateway-Schema

Bevor wir ein Gateway aufsetzen definieren wir einen Namen, dessen Nummer auch gleichzeitig in vielen Scripten genutzt wird.

Mit den uns zugewiesenen Netznummern sowie der Gateway-Nummer und dem Gateway-Namen werden alle benötigten Informationen abgeleitet:

- **IPv4**
  - Für Gateways wird das Subnetz `10.188.255.0/24` verwendet. Die Adressen sind bereits definiert. Beispiel troisdorf1: `10.188.255.1`
- **MAC-Adresse**
  - Privates Prefix (`0a2:8c:ae:6f:f6:**`) + Gatewaynummer
  - **Beispiele:**
    - 10.188.255.1 -> `a2:8c:ae:6f:f6:01`
    - 10.188.255.2 -> `a2:8c:ae:6f:f6:02`
- **IPv6**
  - Range-Prefix (`2a03:2260:121::255:`) + Gatewaynummer
  - **Beispiele:**
    - troisdorf1 -> `2a03:2260:121::255:1/64`
    - troisodrf2 -> `2a03:2260:121::255:2/64`
- **DNS**
  - `troisdorf[1-9].freifunk-troisorf.de` -> A- + AAAA-Record
  - `[1-9].fftdf.de` -> CNAME auf s.o.
  - Reverse DNS Eintrag korrekt setzen für Haupt DNS Namen: `troisdorf[1-9].freifunk-mwu.de`

1.2.7 Beispiel

Gateway: **troisdorf5** - Nummer: **5**

troisdorf5	
IPv4	`10.188.255.5`
IPv6	`2a03:2260:121:5000::5`
MAC	`a2:8c:ae:6f:f6:05`
DNS1	`troisdorf5.freifunk-troisdorf.de`
DNS2	`5.fftdf.de`

1.3 Gluon

Gluon entstand in Lübeck aus dem Bedarf heraus, einheitliche OpenWRT-Images für Freifunk-Nutzer herauszugeben, die bereits vorkonfiguriert und mit allen Packages versehen waren.

Da es nicht nur in Lübeck Freifunk gibt, wurden alle Elemente zusammen getragen, modularisiert, und für alle Freifunk-Communities veröffentlicht. *Vielen Dank!*

Es ist ein Aufsatz, der den normalen OpenWRT Source Code hernimmt, patcht, und anhand der Konfiguration alles zurechtrückt um den OpenWRT-Bauprozess für einen Satz unterstützter Router-Modelle zu starten. Dabei können dem OpenWRT noch weitere Pakete untergeschoben werden.

Heraus fallen fertige Images, vorkonfiguriert, nur noch flashen ist nötig. Bonus: Die Images werden noch fein mit elliptischen Kurven signiert, um ein automatisches Updaten zu ermöglichen (Autoupdater ist ein Standard OpenWRT-Paket für Gluon)

1.3.1 Hintergrund zu Gluon

Ein bisschen zu den Anfängen von Gluon und viel mehr zum technischen Hintergrund kann man unter folgenden Links erfahren:

- http://luebeck.freifunk.net/wiki/gluon (http://luebeck.freifunk.net/wiki/Firmware)
- http://luebeck.freifunk.net/wiki/fastd-schlusselverwaltung
- http://nilsschneider.net/2012/12/24/openwrt-autoupdater.html
- http://nilsschneider.net/2013/02/17/fastd-tutorial.html

1.3.2 Links & Dokumentation

- Gluon Code: https://github.com/freifunk-gluon/gluon
- Gluon Pakete:
  - https://github.com/freifunk-gluon/gluon/tree/master/package
  - https://github.com/freifunk-gluon/packages
- Gluon Konfiguration (site.conf) https://github.com/freifunk-gluon/gluon/tree/master/docs/site-example
- Dokumentation: http://gluon.readthedocs.org/
- Github Wiki: https://github.com/freifunk-gluon/gluon/wiki
- fastd: http://fastd.readthedocs.org/
- Doku aus Hamburg: https://wiki.freifunk.net/Freifunk_Hamburg/Firmware#Gluon

CHAPTER 2

Konfiguration

2.1 Grundkonfiguration

2.1.1 Hostname

Den Hostnamen setzen (ohne Domain):

```
echo "hostname" > /etc/hostname
```

/etc/hosts (am Beispiel von troisdorf5):

```
127.0.0.1   localhost
127.0.1.1   troisdorf5.freifunk-troisdorf.de    troisdorf5

# The following lines are desirable for IPv6 capable hosts
::1     localhost ip6-localhost ip6-loopback
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
5.9.76.198 troisdorf5.freifunk-troisdorf.de troisdorf5
2a01:4f8:161:62a9::5 troisdorf5.freifunk-troisdorf.de troisdorf5
```

2.1.2 Routing Tabellen

/etc/iproute2/rt_tables:

```
#
# reserved values
#
255 local
254 main
253 default
0   unspec
```

```
#
# local
#
#1  inr.ruhep
42 ffrl
```

2.1.3 Pakete

Pakete aus den Standard-Repos installieren:

```
apt-get install -y git make gcc build-essential pkg-config libgps-dev libnl-3-dev␣
↪libjansson-dev isc-dhcp-server collectd libcap-dev iproute libnetfilter-conntrack3␣
↪python-dev libevent-dev ebtables python-virtualenv iptables-persistent iftop screen␣
↪bridge-utils tcpdump bind9 radvd curl htop psmisc dnsutils ntp
```

2.1.4 NTP

Da die Kisten recht viel mit Crypto machen, ist es von Vorteil eine halbwegs genaue Uhrzeit parat zu haben.

Die `/etc/ntp.conf` bleibt nahezu unverändert:

```
# /etc/ntp.conf, configuration for ntpd; see ntp.conf(5) for help

driftfile /var/lib/ntp/ntp.drift

# Specify one or more NTP servers.
server 0.de.pool.ntp.org
server 1.de.pool.ntp.org
server 2.de.pool.ntp.org
server 3.de.pool.ntp.org

# Use Ubuntu's ntp server as a fallback.
server ntp.ubuntu.com

# By default, exchange time with everybody, but don't allow configuration.
restrict -4 default kod notrap nomodify nopeer noquery
restrict -6 default kod notrap nomodify nopeer noquery

# Local users may interrogate the ntp server more closely.
restrict 127.0.0.1
restrict ::1
```

2.2 Netzwerk Interfaces

/etc/network/interfaces

Hier richten wir hauptsachlich die GRE Tunnel zum FFRL ein.

The loopback network interface auto lo iface lo inet loopback

up ip address add 185.66.193.105/32 dev lo

iface lo inet6 loopback up ip address add 2a03:2260:121::105/48 dev lo

The primary network interface allow-hotplug eth0 iface eth0 inet dhcp allow-hotplug eth1 iface eth1 inet6 static

address 2a01:4f8:161:62a9::5 netmask 64 gateway 2a01:4f8:161:62a9::2

GRE Tunnel zum Rheinland Backbone # - Die Konfigurationsdaten werden vom Rheinland Backbone vergeben und zugewiesen

Berlin Router A auto gre-bb-a.ak.ber iface gre-bb-a.ak.ber inet static

address 100.64.2.151 netmask 255.255.255.254 pre-up ip tunnel add $IFACE mode gre local 5.9.76.198 remote 185.66.195.0 ttl 255 post-up ip link set $IFACE mtu 1400 post-down ip tunnel del $IFACE

iface gre-bb-a.ak.ber inet6 static address 2a03:2260:0:155::2/64 netmask 64

Berlin Router B auto gre-bb-b.ak.ber iface gre-bb-b.ak.ber inet static

address 100.64.2.153 netmask 255.255.255.254 pre-up ip tunnel add $IFACE mode gre local 5.9.76.198 remote 185.66.195.1 ttl 255 post-up ip link set $IFACE mtu 1400 post-down ip tunnel del $IFACE

iface gre-bb-b.ak.ber inet6 static address 2a03:2260:0:156::2/64 netmask 64

Duesseldorf Router A auto gre-bb-a.ix.dus iface gre-bb-a.ix.dus inet static

address 100.64.2.155 netmask 255.255.255.254 pre-up ip tunnel add $IFACE mode gre local 5.9.76.198 remote 185.66.193.0 ttl 255 post-up ip link set $IFACE mtu 1400 post-down ip tunnel del $IFACE

iface gre-bb-a.ix.dus inet6 static address 2a03:2260:0:157::2/64 netmask 64

Duesseldorf Router B auto gre-bb-b.ix.dus iface gre-bb-b.ix.dus inet static

address 100.64.2.157 netmask 255.255.255.254 pre-up ip tunnel add $IFACE mode gre local 5.9.76.198 remote 185.66.193.1 ttl 255 post-up ip link set $IFACE mtu 1400 post-down ip tunnel del $IFACE

iface gre-bb-b.ix.dus inet6 static address 2a03:2260:0:158::2/64 netmask 64

2.3 DNS-DHCP-IP

2.3.1 BIND

/etc/bind/named.conf.fftdf:

zone "fftdf" { type slave; masters { 10.188.1.100; }; file "/var/lib/bind/db.fftdf";

};

/etc/bind/named.conf.options

options { directory "/var/cache/bind";

// If there is a firewall between you and nameservers you want // to talk to, you may need to fix the firewall to allow multiple // ports to talk. See http://www.kb.cert.org/vuls/id/800113

// If your ISP provided one or more IP addresses for stable // nameservers, you probably want to use them as forwarders. // Uncomment the following block, and insert the addresses replacing // the all-0's placeholder.

// forwarders { // 0.0.0.0; // };

```
        //========================================================================
        // If BIND logs error messages about the root key being expired, //
        you will need to update your keys. See https://www.isc.org/bind-keys
        //========================================================================
        dnssec-validation auto;

        auth-nxdomain no; # conform to RFC1035 listen-on { 10.188.255.5; }; listen-on-v6 {
        2a03:2260:121::255:5; };

};
```

2.3.2 DHCPd

Um IPv4 im Netzwerk nutzen zu können müssen wir auf dem Gateway einen DHCP Server aufsetzen. Der DHCP Server Verteilt die Adressen aus dem zum Gateway zugewiesenen Adressbereich.

See also:

Netzplan

Die Konfiguration ist relativ einfach gehalten. Sie wird unter /etc/dhcp/dhcpd.conf abgelegt:

```
ddns-update-style none; option domain-name “fftdf”; default-lease-time 300; max-lease-time 3600;
log-facility local7; subnet 10.188.0.0 netmask 255.255.0.0 { authoritative; range HIER DER RANGE
AUS DEM NETZPLAN; option domain-name-servers 10.188.255.5; option routers 10.188.255.5; option
interface-mtu 1312; interface bat0; }
```

TBD

2.4 RAdvD

Damit die Clients im Netz auch in den Genuss von öffentlichem IPv6 kommen, müssen die Public IPv6-Prefixe zusätzlich zu den ULA-Prefixes per Router Advertisements bekannt gegeben werden. Dazu ergänzt man die Public IPv6-Prefixe in der /etc/radvd.conf:

```
interface bat0 { AdvSendAdvert on; IgnoreIfMissing on; MaxRtrAdvInterval 200; RDNSS
    2a03:2260:121::255:5 {}; prefix 2a03:2260:121::/64 {

        AdvOnLink on; AdvAutonomous on; AdvRouterAddr on;

    };

};
```

2.5 A.L.F.R.E.D.

TBD

2.6 Internet-Exit

TBD

2.6.1 Freifunk Rheinland e.V.

TBD

CHAPTER 3

Betrieb

CHAPTER 4

Firmware

4.1 v1.0

See also:

Github site.conf

- Erstes Gluon Release nach dem Netsplit

4.2 v1.0.2

See also:

Github site.conf

- Anpassung der IPv6 Adressen in den neuen netzen

4.3 v1.0.3

See also:

Github site.conf

Autoupdater Bugfix

4.4 v1.0.5

See also:

Github site.conf

- Bugfixes

4.5 v1.0.7

See also:

Github site.conf

- Fehlerbehebungen im Reboot und Wifi Restart Script

4.6 v2017.1.1-1

See also:

Github site.conf

- Änderrung Versionsnummern auf [GLUON-VERSION]-[BUILD-NUMMER]
- Gluon Release 2017.1.1

4.7 v2017.1.2-1

See also:

Github site.conf

- Gluon Release 2017.1.2

4.8 v2017.1.3-1

See also:

Github site.conf

- Gluon Release 2017.1.3

4.9 v2017.1.4-1

See also:

Github site.conf

- Täglicher reboot in Wöchentlichen Reboot geändert
- Täglicher reboot wenn keine Clients auf dem Node sind um 4 Uhr
- ATK10 Images werden wieder gebaut
- Gluon Release 2017.1.4

See also:

Github site.conf

- Update auf Gluon Master wegen Wifi Problemen

CHAPTER 5

Mitwirken

Du hast eine Stelle entdeckt, die Schreibfehler enthält, was unsauber oder falsch erklärt, nicht existiert aber sollte, oder veraltet ist?

Gerne nehmen wir sinnvolle Vorschläge und Ergänzungen mit auf, über den Issue-Tracker (mit dem Label ‘Doku’) oder am besten gleich per Pull Request.