Die L3 Transition von Freifunk Franken

KNF-Kongress 2015

Tim Niemeyer <tim@freifunk-franken.de>

https://github.com/RedDog99/vortrag-knf.git
f7ec013

22.11.2015

Inhalt

Freifunk

Freifunk

- Offenes WLAN
  - Wireless-Adhoc-Mesh Netzwerk
- Lokaler Ableger der Freifunk-Bewegung (freifunk.net)
- Nicht-kommerzielle Initiative für freie Funknetzwerke
  - → Bürger investieren in Eigenregie Zeit, Geld und Enthusiasmus
- Mehr als „kostenloses Internet“:
  - Unabhängiges / dezentrales Netz
  - Internet Technologie beim Bürger
  - → Freies Netzwerken
- `(Irgendwann mal Teil vom Internet?)`

Das braucht man

- Einen günstigen, unterstützten Router (ab ca. 17€)
- Eine spezielle Firmware
- Die Zustimmung zum „Pico-Peering Agreement“[1]:
  1. Freier Transit
  2. Offene Kommunikation
  3. Keine Garantie (Haftungsausschluss)
  4. Nutzungsbestimmungen
  5. Lokale (individuelle) Zusätze

[1] Regelwerk, über grundsätzliche Eigenschaften des Freifunks

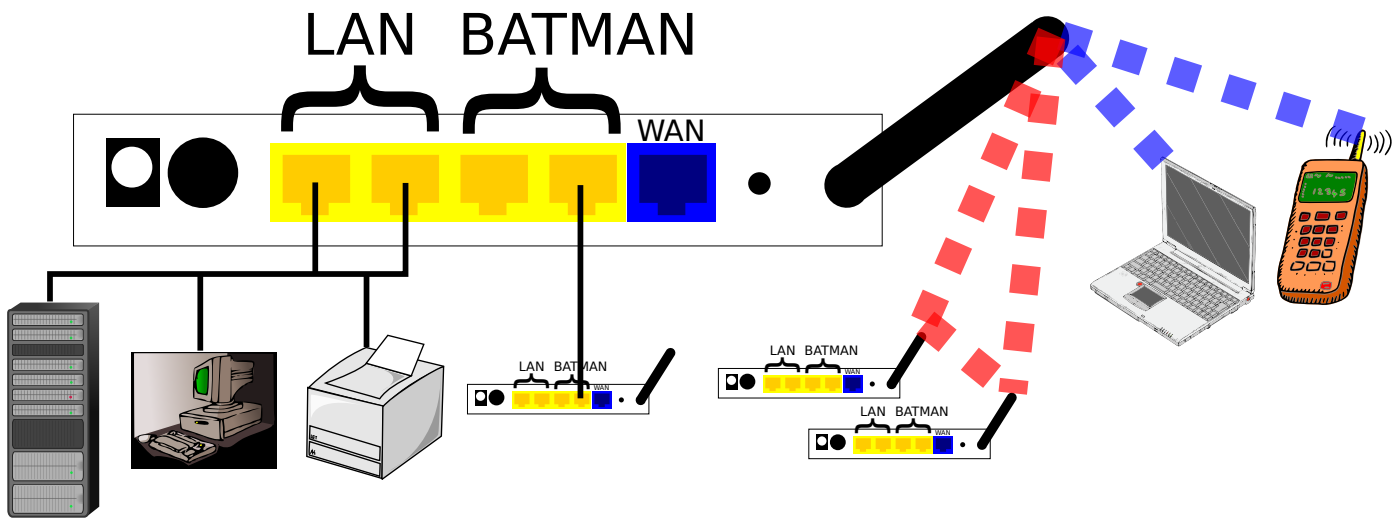
Grundlagen

Ein typisches Freifunk Netz

- Ein Batman-Adv Netz
  - → ”Wie ein großer dezentraler Switch”
- VPN (fastd) für die Funkinseln
  - Multi-Client zu Multi-Client VPN
  - Kein internes Routing
  - Kein Forwarding
  - Layer-II Netz
- Mehrere VPN Server / Gateway
  - DHCP
  - DNS Namensauflösung
  - Gateway zum Internet / ICVPN
    - z. B. mittels Policy-based routing
- Monitoring
  - Karte aller Knoten

Freifunk Router (aussen)

- Client-Ports & Infrastructure Funknetz: Wie ein großer Switch
- Batman-Ports & Ad-Hoc Funknetz: Mesh-Netz
- WAN-Ports: VPN Netz

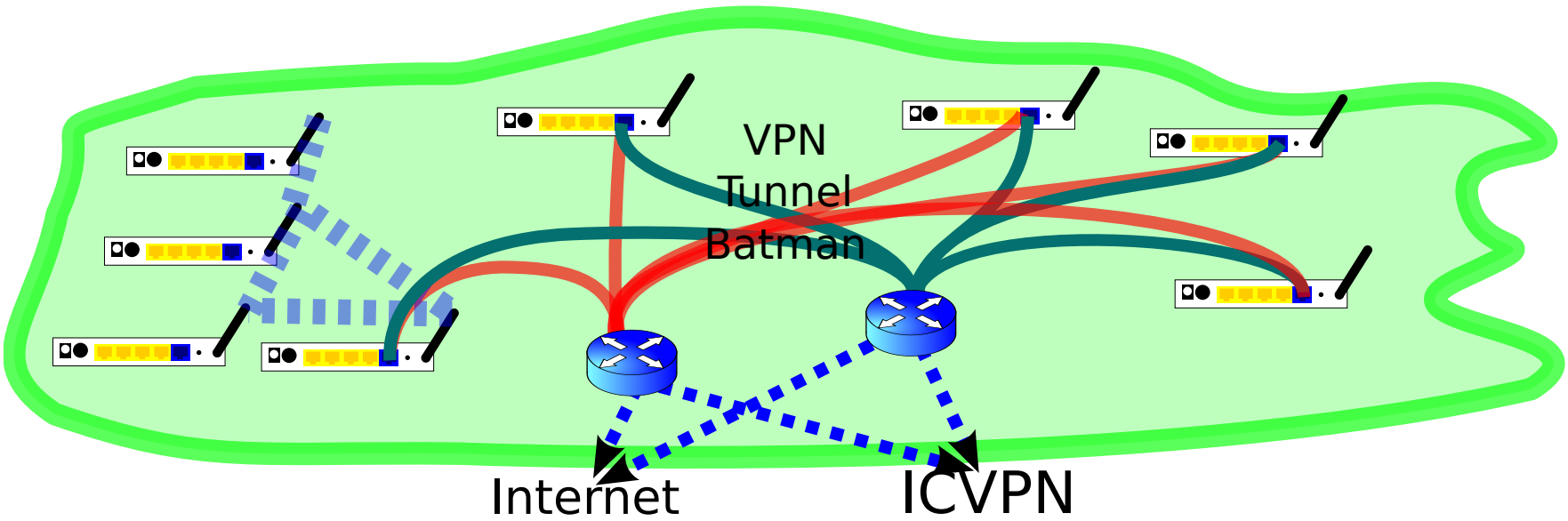


Freifunk Router (innen)

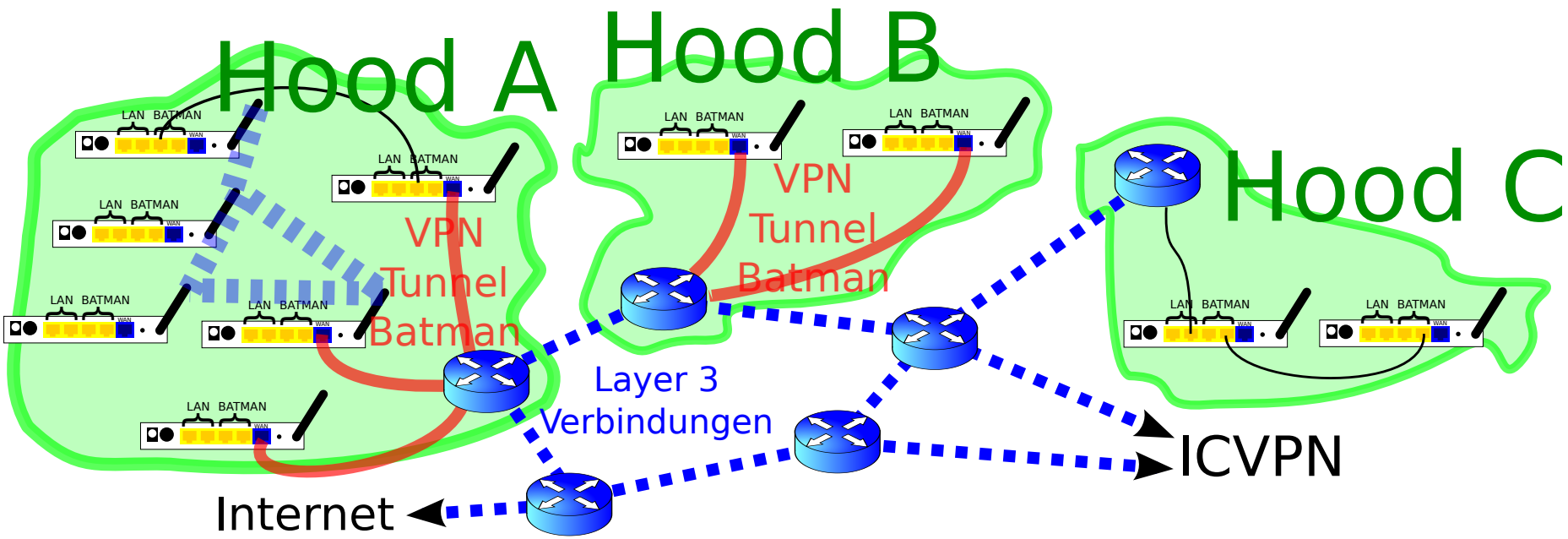
- OpenWrt
- Batman-Adv
- Fastd Client
- Monitoring Daten (Nodewatcher / Alfred)
- .. kleinere Tools / Configs / Skripte

<table>
<tr><td colspan="6">Bridge</td></tr>
<tr><td rowspan="2">Managed</td><td colspan="3">B.A.T.M.A.N</td><td rowspan="2" colspan="2">Client-VLan</td></tr>
<tr><td>Ad-Hoc</td><td>VPN</td><td colspan="2">Node-VLan</td></tr>
<tr><td colspan="2">WiFi</td><td>WAN</td><td>LAN1</td><td>LAN2</td><td>LAN3</td><td>LAN4</td></tr>
</table>

Ein typisches Freifunk Netz



Unser grobes Ziel



- Mehrere Layer-2 Inseln (Hoods)
- Verbindung per Layer-3
- Dezentrale Gateways

Stand von heute

Freifunk Knoten

- Ziel: Ohne Konfiguration
  - Keine DHCP Ranges
  - LAN Ports vorkonfiguriert
  - Ausnahme: Passwort für root Login
- Hat nur eine Link-Local IPv6 Adresse
- Nur SSH Zugang

  → Kein Webinterface
- Batman-Adv 2013 (!)

Knoten VPN

- Verwendetes VPN: fastd
- Wir nutzen keine Verschlüsselung (! :-O)
- Script zum Austausch der VPN Peers über den KeyXchange

VPN-KeyXchange

- Zentrale Webseite
- Knoten meldet sich beim VPN-KeyXchange an
- Knoten lädt Liste mit Peers
- Knoten Identifizierung über MAC, alternativ über Name

VPN-KeyXchange

- Zentrale Webseite
- Knoten meldet sich beim VPN-KeyXchange an
- Knoten lädt Liste mit Peers
- Knoten Identifizierung über MAC, alternativ über Name
- Aufteilung in ,,hood”s:
  - Die Hood, welche am nächsten dran ist (voronoi) wird zugewiesen
    - Standort des Routers wird im Netmon anhand der MAC ermittelt
    - Problem: Abhängigkeit vom Netmon
  - Clients bekommen eine Liste aller Server
  - Server bekommen eine Liste aller Clients+Server
- Problem: Funk Verbindung zwischen den Hoods

VPN Server

- VPN Server: In jeder Hood gibt es mehrere davon
- Hoodzuweisung manuell im KeyXchange
- DHCP
  - Aktuell ausschließlich IPv4
  - Ungleiche Server Auslastung durch schlechtes DHCP Timing
  - Batman-Adv GW Selection
- DNS Namesauflösung
- Policy base routing
- VPN (GRE) Tunnel zu anderen Gateways
- OLSR
  - Routing zu anderen Gateways

Gateways

- Verbindet Freifunk und Internet
- IPv4 NAT (oft übers Ausland) ins Internet
- Announced 0.0.0.0/0 via OLSR
  - Dynamic Gateway Plugin
  - VPN Server können diese Routen nutzen
  - Problem: Ungleiche Server Auslastung durch statische Routen-Qualität

Netmon

- Nodewatcher
  - Generiert Status-Daten
  - XML
  - alle 5 Minuten
- Configurator
  - Verknüpft Netmon und Knoten
- Crawler
  - Sammelt Status-Daten
  - Download über http Schnittstelle der Knoten
  - Alles über Link-Local
    - Muss in jeder Hood drin sein
- Netmon
  - Visualisiert Status-Daten
  - Mit den vielen Crawls hoffnungslos überfordert

Monitoring

- Alfred
  - XML
  - alle 5 Minuten
  - Multicast
- Multicast Daten können auf mehreren Gateways gelesen werden
- Die Daten können von dort an eine zentrale Webseite (Karte, etc.) geschickt werden
- Standort und Ansprechpartner wird aus dem Netmon geladen
- Problem: Abhängig vom Netmon

Domain-Name-System

- ganz Neu.. ! :-)
- fff.community
  - Langer Name, aber
  - Keine Kollision
- Mehrere DNS Server
- Zonen-Synchronisation über dig axfr
- Subdelegation an synchronisierte Hosts möglich
- Noch keine reverse delegation

Firmware Bau

- Basiert auf OpenWrt
- ,,Eigenes” Framework (Buildscript)
- Zentrales ,,files” Verzeichnis
- Board-Support-Packages
  - Ein .config
  - Überschreibende ,,files”
- Template System für versch. Communities

Zusammenfasssung

- Erfolgreich das L2 Netz in mehrere L3 Netze geteilt
- VPN Schlüsseltausch über zentrales Tool
  - Zuordnung zu Hood über Standort aus Netmon
  - Manuelle Zuweisung der VPN Server
  - Keine Anpassung an Firmware
    - Fehlerhafte Verbindung (loop) der Hoods durch versehentliches Meshing
- Kein Traffic Balancing zwischen VPN Server und Gateways
- Netmon überlastet
- Netmon muss zu jeder Hood eine L2 Verbindung haben
- Neues Monitoring kennt Knoten Standort nur über Netmon
- Keine Möglichkeit die L2 Netze per Richtfunk zu verbinden

Mögliche Lösungen

Größten Baustellen

Größere (längerfristige) Baustellen:

- Netmon soll weg
- KeyXchange soll dezentralisiert werden
- Funk Verbindungen zwischen Hoods

Monitoring

- Netmon abschalten, Abhängigkeiten lösen
  - keyXchange
  - neues Monitoring
- Position und Owner Daten vom Gerät
- Webinterface nötig

Webinterface

- z. B. mit haserl (Freifunk Bielefeld)
- z. B. mit lua (OpenWrt)
- Parameter setzen
  - Koordinaten setzen
    - Lösung gesucht: Kartenansicht ohne Netz?
  - Kontakt-Daten
- Problem: ”GUI” Browser und IPv6 Link-Local

IP für Knoten

- Knoten müssen eine normale IP bekommen
- DHCP IP immer anders $\rightarrow$ wie Router finden?
  - Dynamic DNS: MAC.node.fff.community
    - Muss schnell gehen $\rightarrow$ DHCP setzt das Dynamic DNS
    - Problem: offline Knoten
  - Local-Node IP:
    - Jeder Knoten hat die selbe IP
    - Beispiel: Vom DHCP zugewiesene Netzadresse +127
    - Local-Node IP wird nicht ins Mesh geroutet
    - Problem: Geht nur bei größeren Netzen
  - IP im Monitoring nachschlagen
    - Problem: offline Knoten
- Local Node mit ebtables?

KeyXchange

- Dezentralisieren: Knoten soll selber seine Hood finden
  - VPN Server auswählen
  - VPN Server alle Verbindungen akzeptieren
- WiFi Settings auswählen
  - Problem: wenn z.B. kein VPN da ist?
- Zwei Dinge werden benötigt:
  - Mögliche VPN Server
  - Daten der Hood (WiFi / Routing / etc)

Hood-Configs

Hood Config

```
[general]
version=1

[hood]
name=fuerth
bssid=ca:ff:ee:ba:be:00
protocol=batman-adv-v14
channel2=1
mode2=ht20+
type=802.11s
location=49.4814;10.966
noAutoConnect=true

[network]
subnet=10.16.44.0/27
```

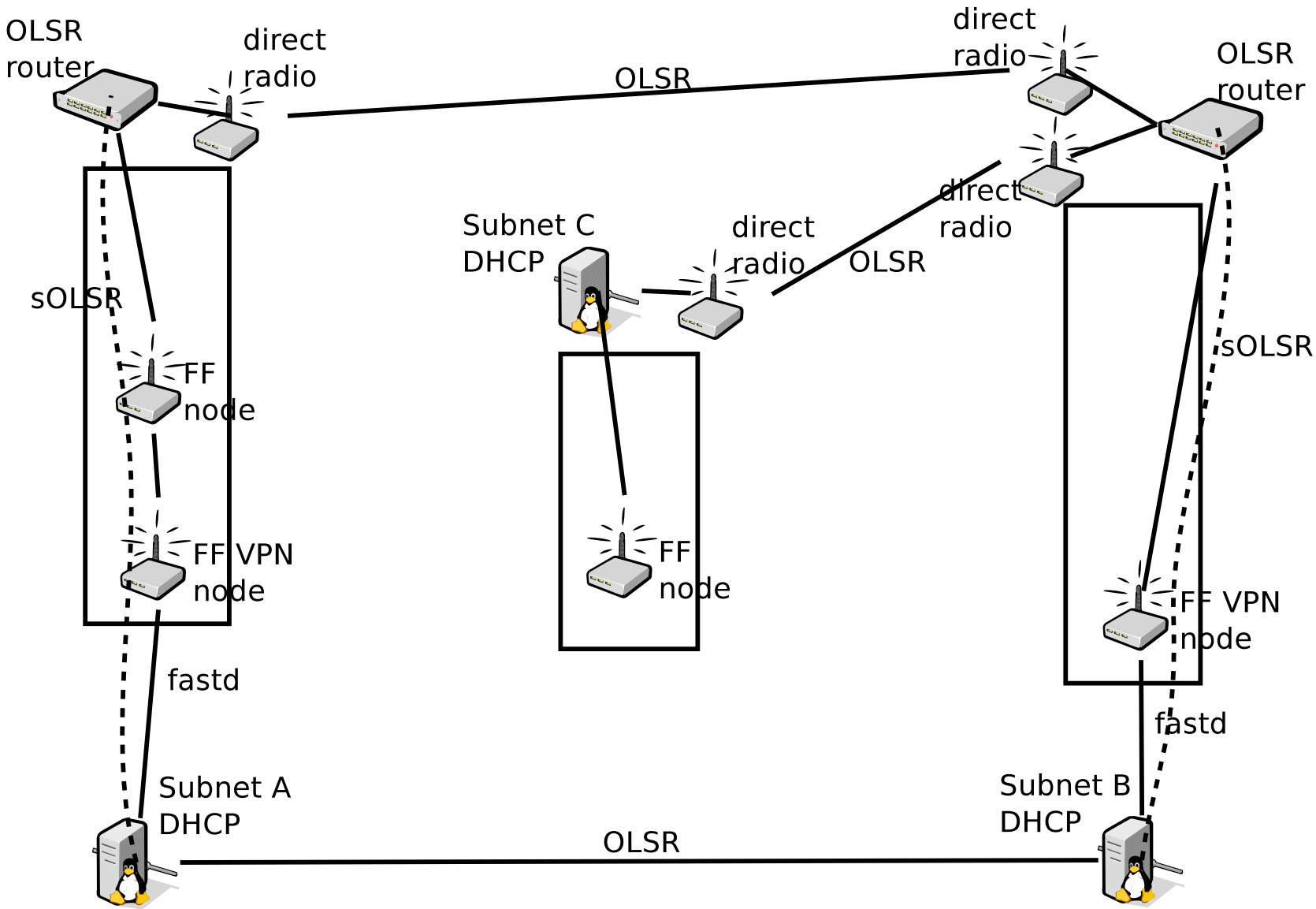
Gateway Config

```
[general]
version=1

[network]
hood=fuerth
ip4range=10.50.44.1-.46.255
//ip6range=2001:xx:xx:xx/64

[vpn]
protocol=fastd
address=vpn1.fff.community
port=10000
key=<fastd-public-key>

[sign]
key=<public-key>
```

Hood-Configs verteilen

- Gesucht: Synchronisation
- Überschreiben/Löschen absichern
  - → Synchronisation nur mit Signatur
- Offline Hood
  - Mögliche Funkpartner finden
  - WiFi suchen
  - → Zwei WiFi
    - Mit Freifunk
    - Ohne Freifunk

L3 Richtfunk



L3 Richtfunk

- Batman Netz = Normales Ethernet
- OLSR gegen Unfug absichern $\rightarrow$ sOLSR (??)
- Problem: Nur ein default Gateway pro Client
  - $\rightarrow$ Das Gateway vom Dach oder das hinter dem DSL?

Ende

Vielen Dank für Eure Aufmerksamkeit ...