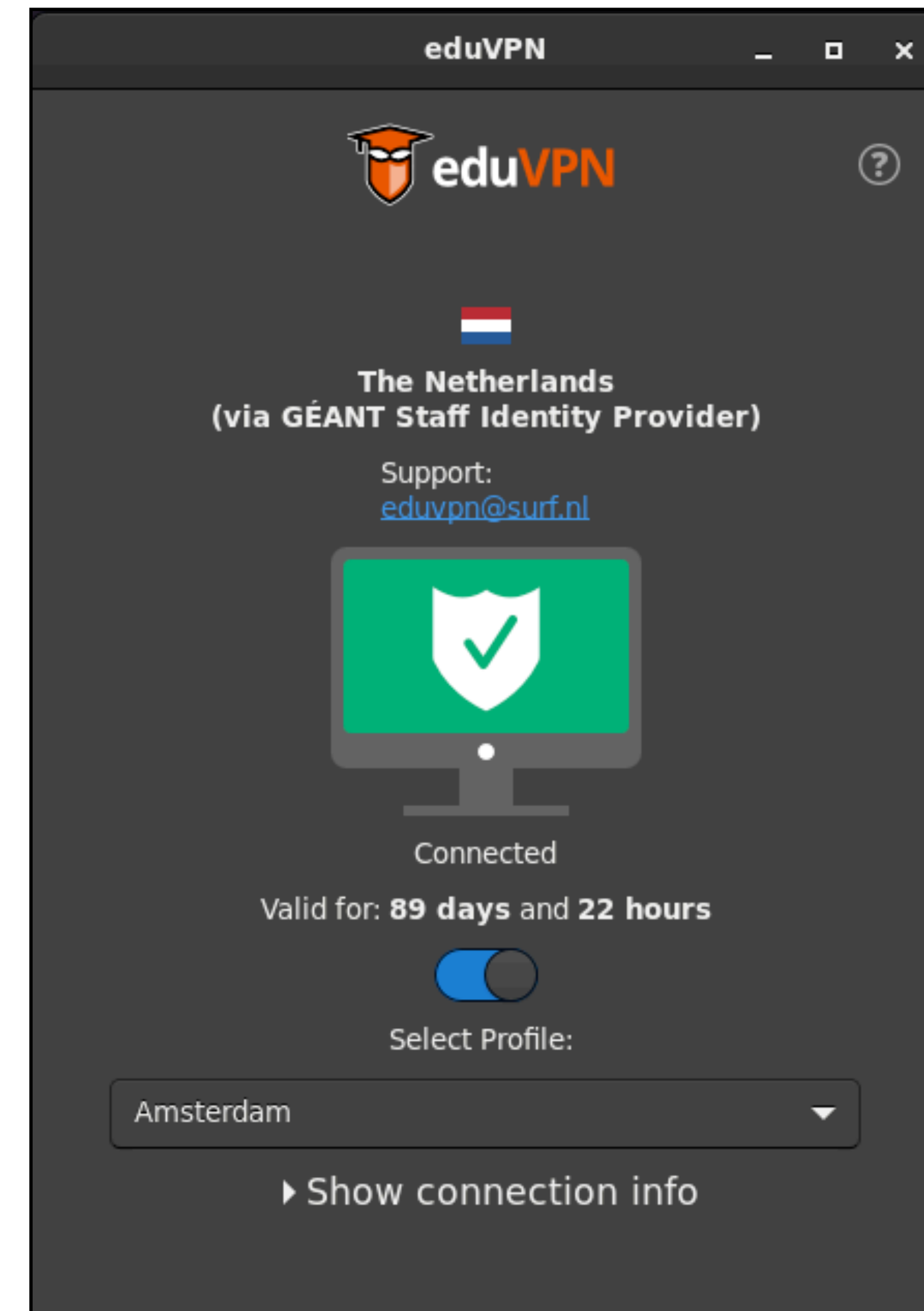# ProxyGuard
WireGuard behind a reverse proxy

Jeroen Wijenbergh, 2nd of February 2025 FOSDEM, Network track

Me

eduVPN

- Free & open-source VPN

- Focused on research & education

- Easy to self-host: https://docs.eduvpn.org/server/v3/

- Supports OpenVPN & WireGuard (since version 3)

- OpenVPN has UDP + TCP out of the box

- WireGuard only UDP

So what?

- UDP can be blocked ☹️

- MTU issues

- 443/53 not the holy grail

- Less is more: 4,000 LOC [1], compared to OpenVPN's 70,000 [2]

- Missing features: TCP

- Quote: *Transforming WireGuard's UDP packets into TCP is the job of an upper layer of obfuscation* https://wireguard.com/known-limitations/

1: https://www.wireguard.com/papers/wireguard.pdf

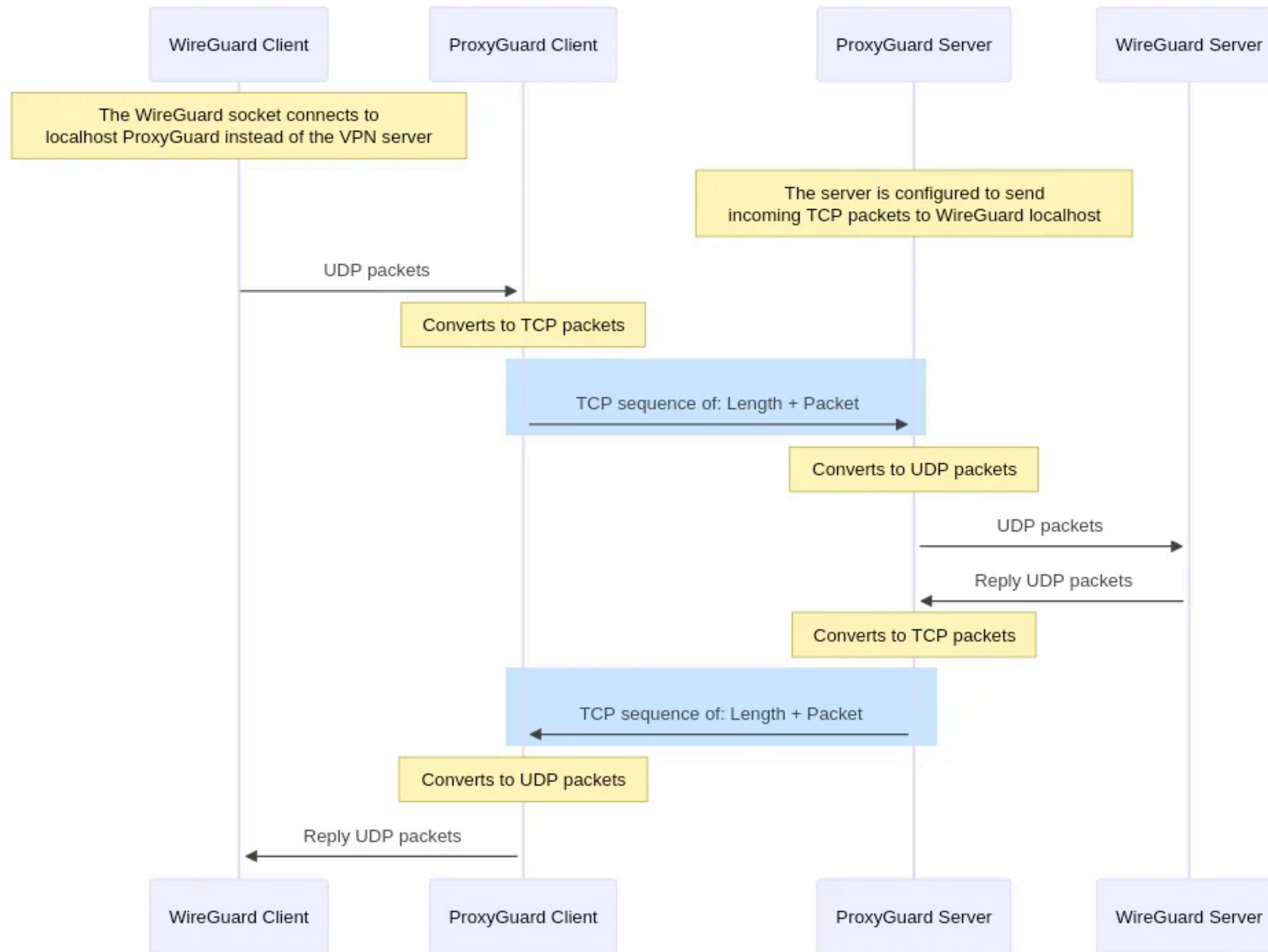2: https://blog.openvpn.net/what-is-cloudflare-vpn/

Finding a tool

- Must: Client & Server implementation

- Nice to have:

  - Go implementation 🐹

  - Run behind reverse proxy (port sharing) 🏃

  - TLS

ProxyGuard

- https://codeberg.org/eduvpn/proxyguard

- First version in Go

- Simple UDP wrapper over TCP

- How to deal with cut-off packets?

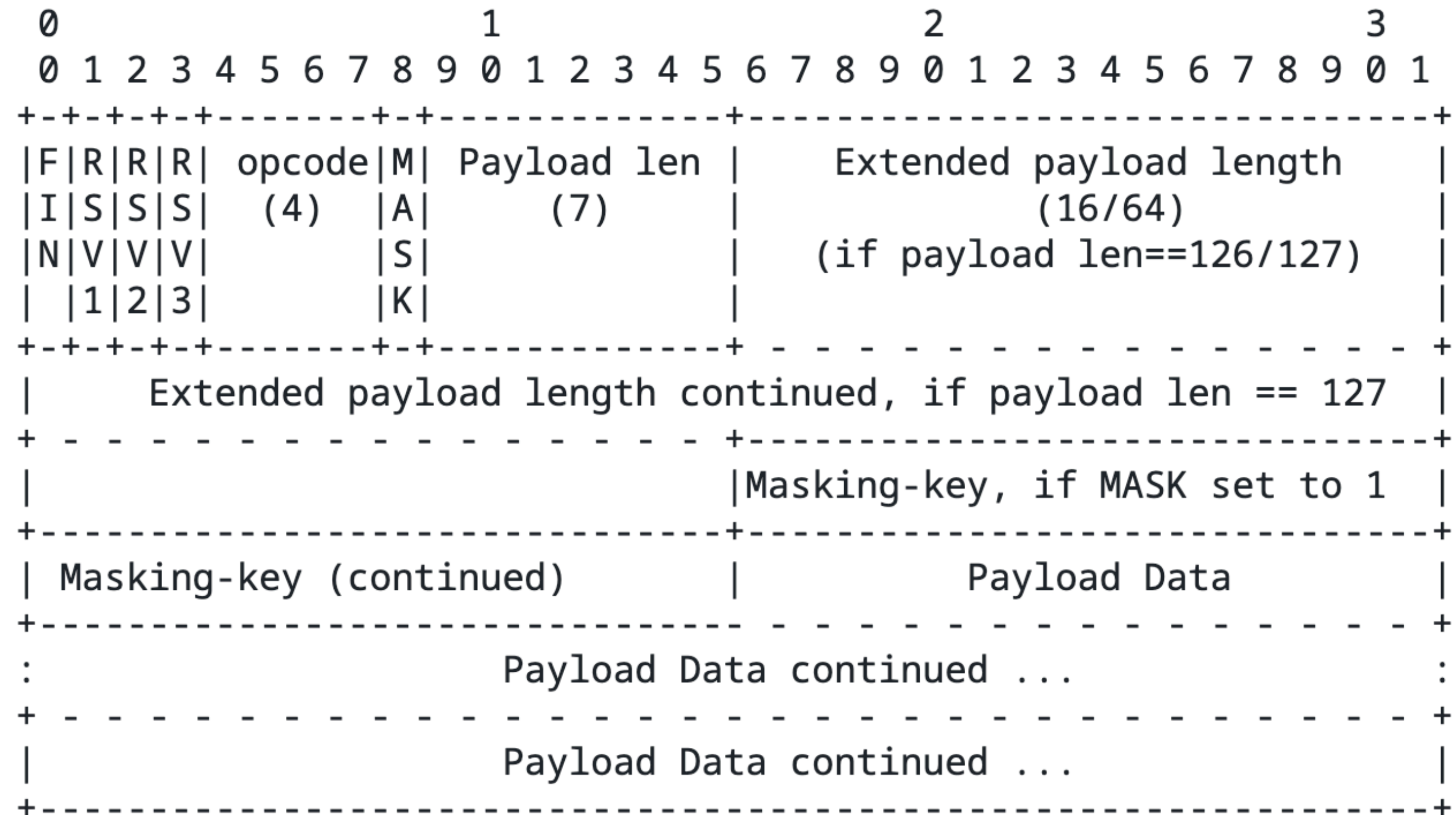# Checking the requirements

- ✅ Client & Server implementation

- Nice to have:

  - ✅ Go implementation

  - ❌ Run behind reverse proxy (port sharing)

  - ❌ TLS

Reverse proxy?

- Need to somehow proxy the connection?

- WebSockets?
  - Complex packet format
  - Does more than we need

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-------+-+-------------+-------------------------------+
|F|R|R|R| opcode|M| Payload len |    Extended payload length    |
|I|S|S|S|  (4)  |A|     (7)     |             (16/64)           |
|N|V|V|V|       |S|             |   (if payload len==126/127)   |
| |1|2|3|       |K|             |                               |
+-+-+-+-+-------+-+-------------+ - - - - - - - - - - - - - - - +
|     Extended payload length continued, if payload len == 127  |
+ - - - - - - - - - - - - - - - +-------------------------------+
|                               |Masking-key, if MASK set to 1  |
+-------------------------------+-------------------------------+
| Masking-key (continued)       |          Payload Data         |
+-------------------------------+ - - - - - - - - - - - - - - - +
:                     Payload Data continued ...                :
+ - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - +
|                     Payload Data continued ...                |
+---------------------------------------------------------------+
```

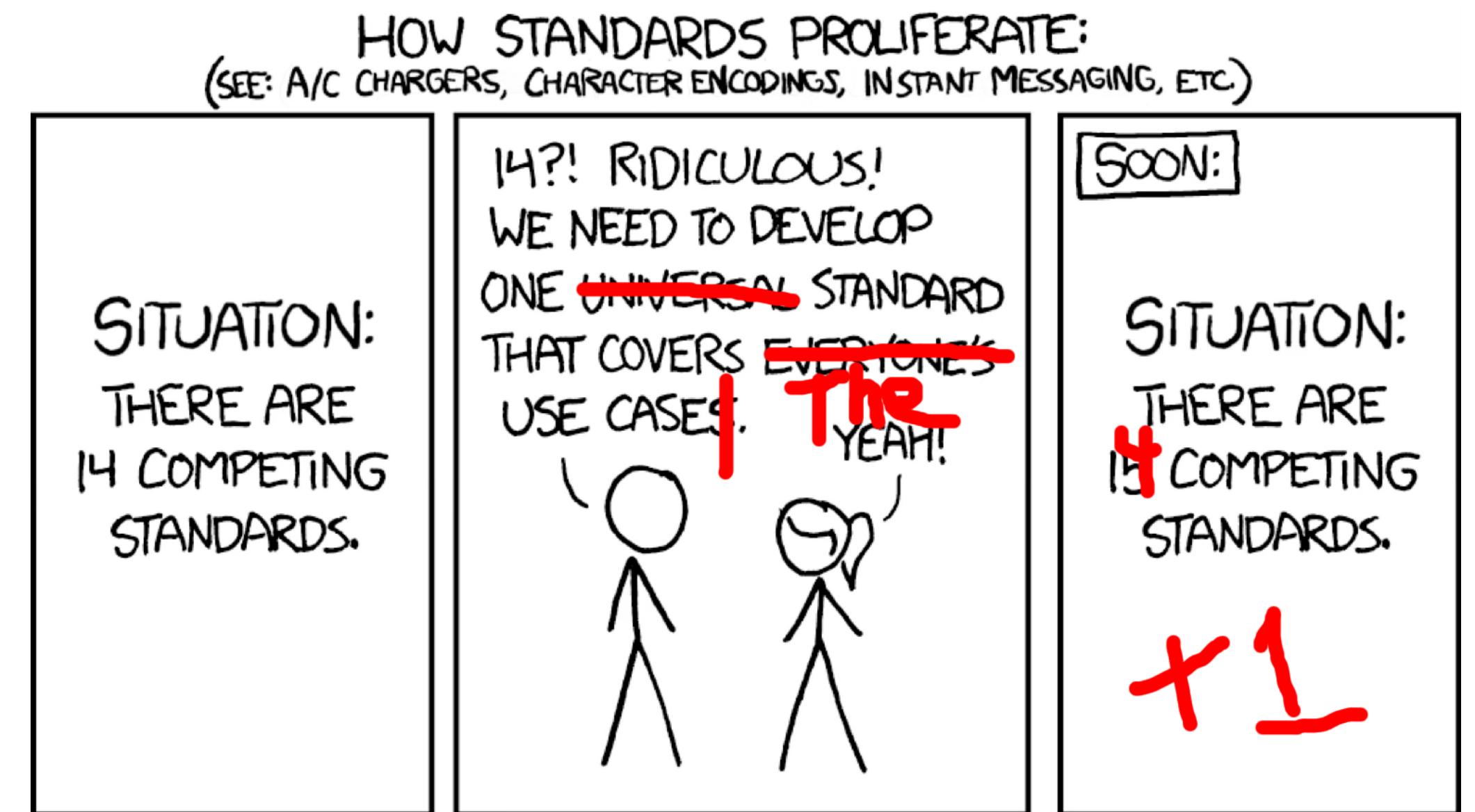https://datatracker.ietf.org/doc/html/rfc6455

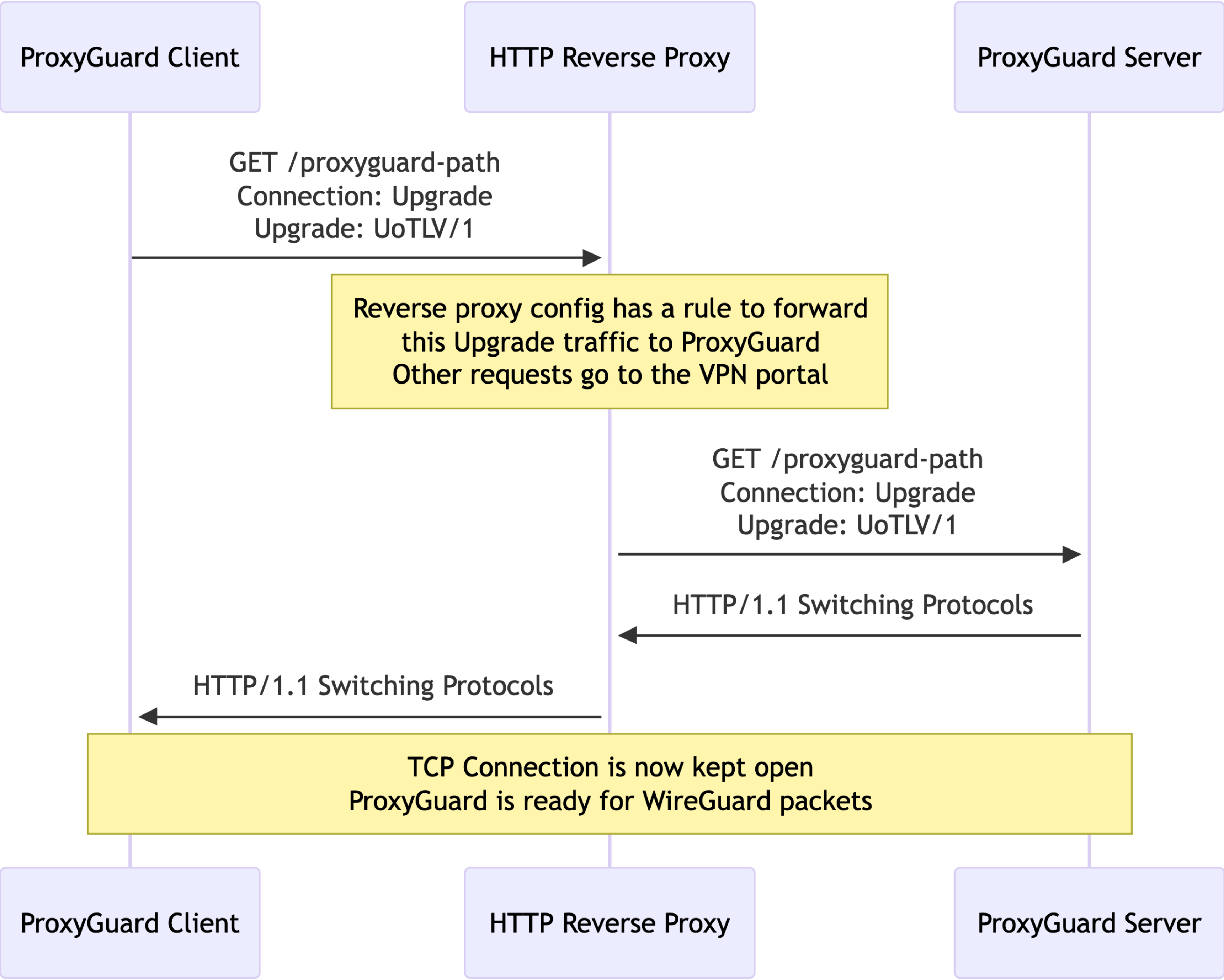# Fine, our own protocol?!

- Idea:
  - Re-use the handshake of web-sockets
 - Keep the packet format length + value
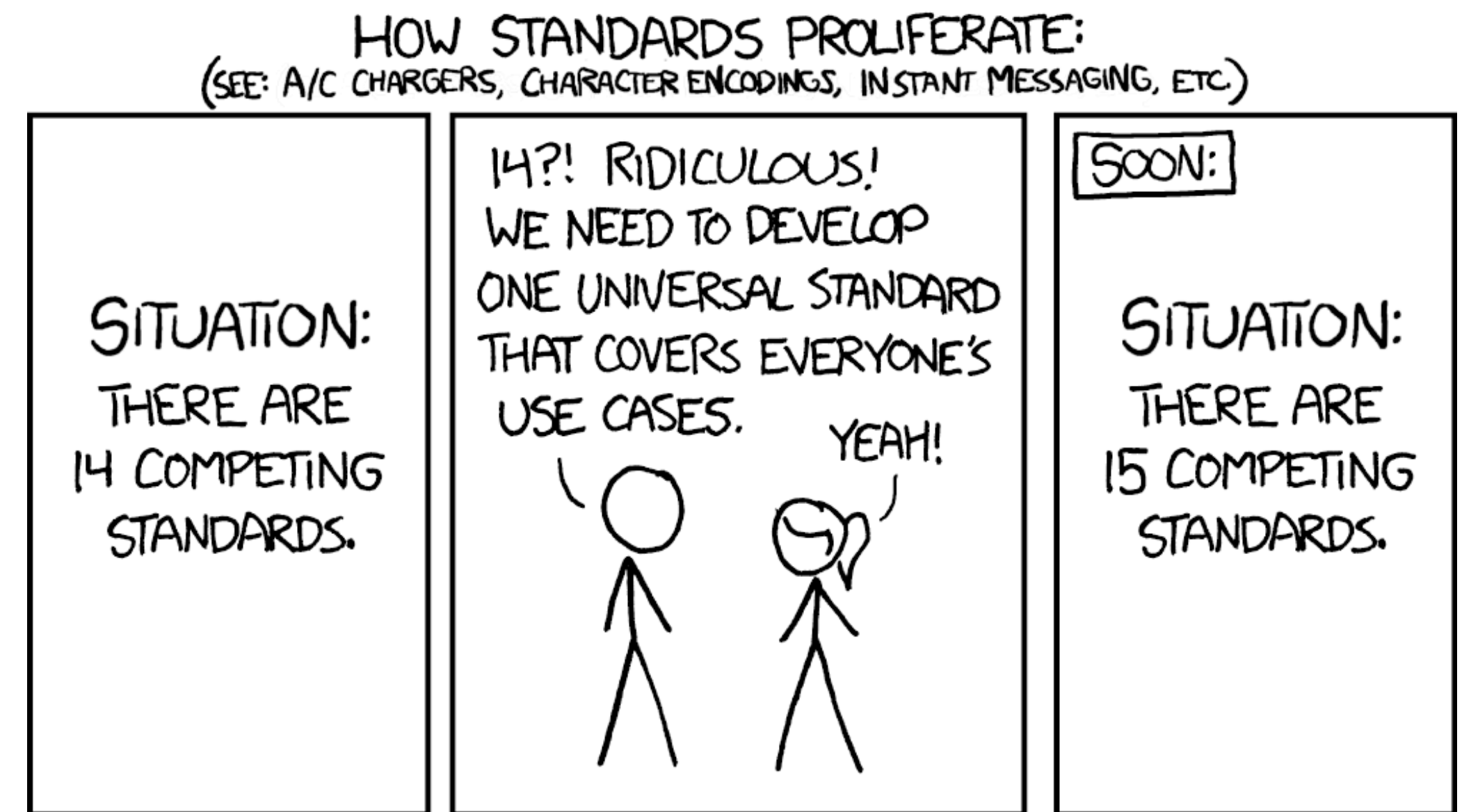
Fine, our own protocol?!

- Idea:
  - Re-use the handshake of web-sockets
  - Keep the packet format length + value

dev@dev-QEMU-Virtual-Machine: ~

dev@dev-QEMU-Virtual-Machine: ~ ✕   dev@dev-QEMU-Virtual-Machine: ... ✕   dev@dev-QEMU-Virtual-Machine: ... ✕   debian@debian: ~ ✕

```
[Interface]
PrivateKey = ...
Address = ...
DNS = ...
ListenPort = 51820
Fwmark = 51820

[Peer]
PublicKey = ...
AllowedIPs = 0.0.0.0/0,::/0
PersistentKeepalive = ...
# ProxyGuard client listener
Endpoint = 127.0.0.1:51821
~
~
~
                              7,0-1                    All
```

ProxyGuard: Client implementations

https://codeberg.org/amebis/wireguard-windows
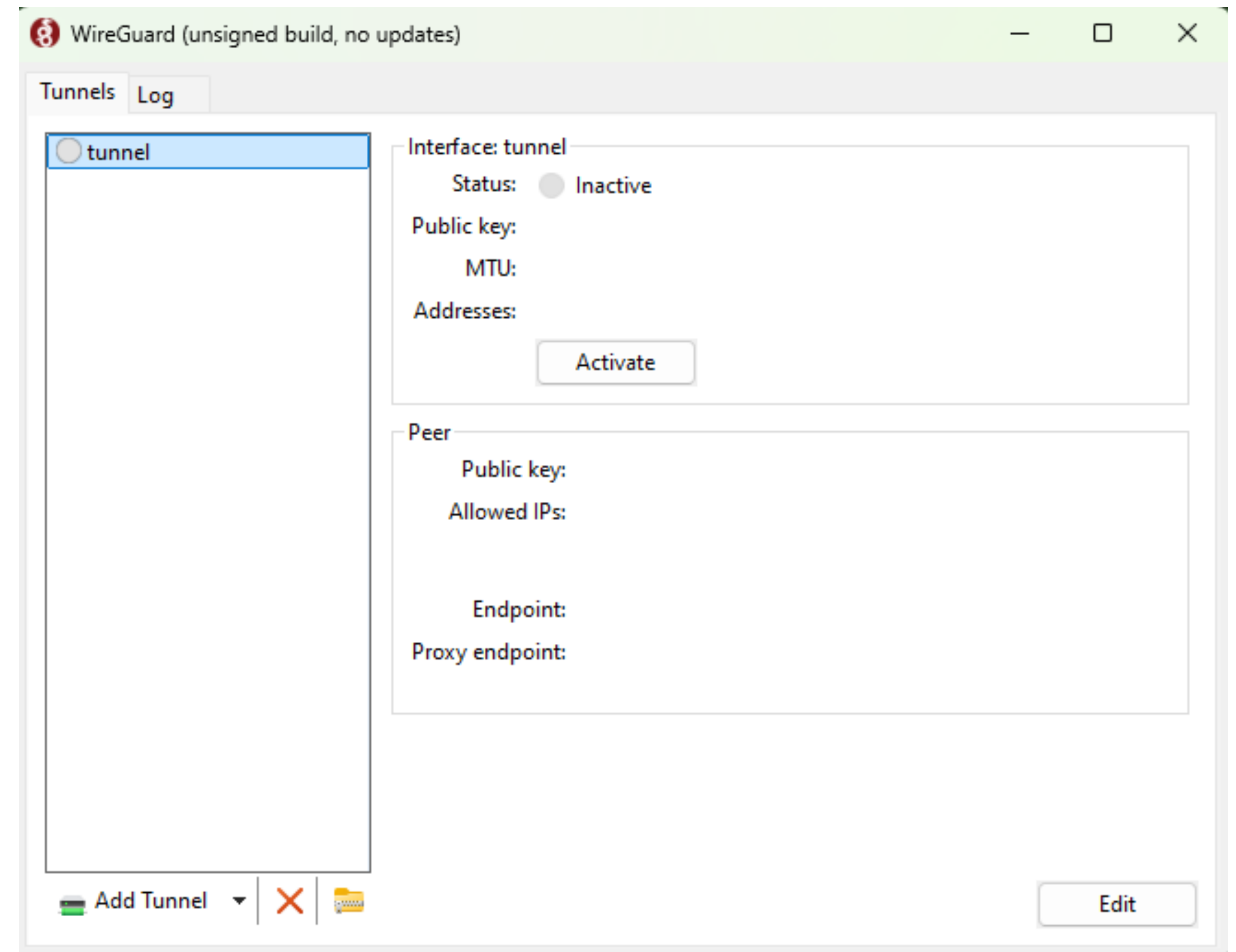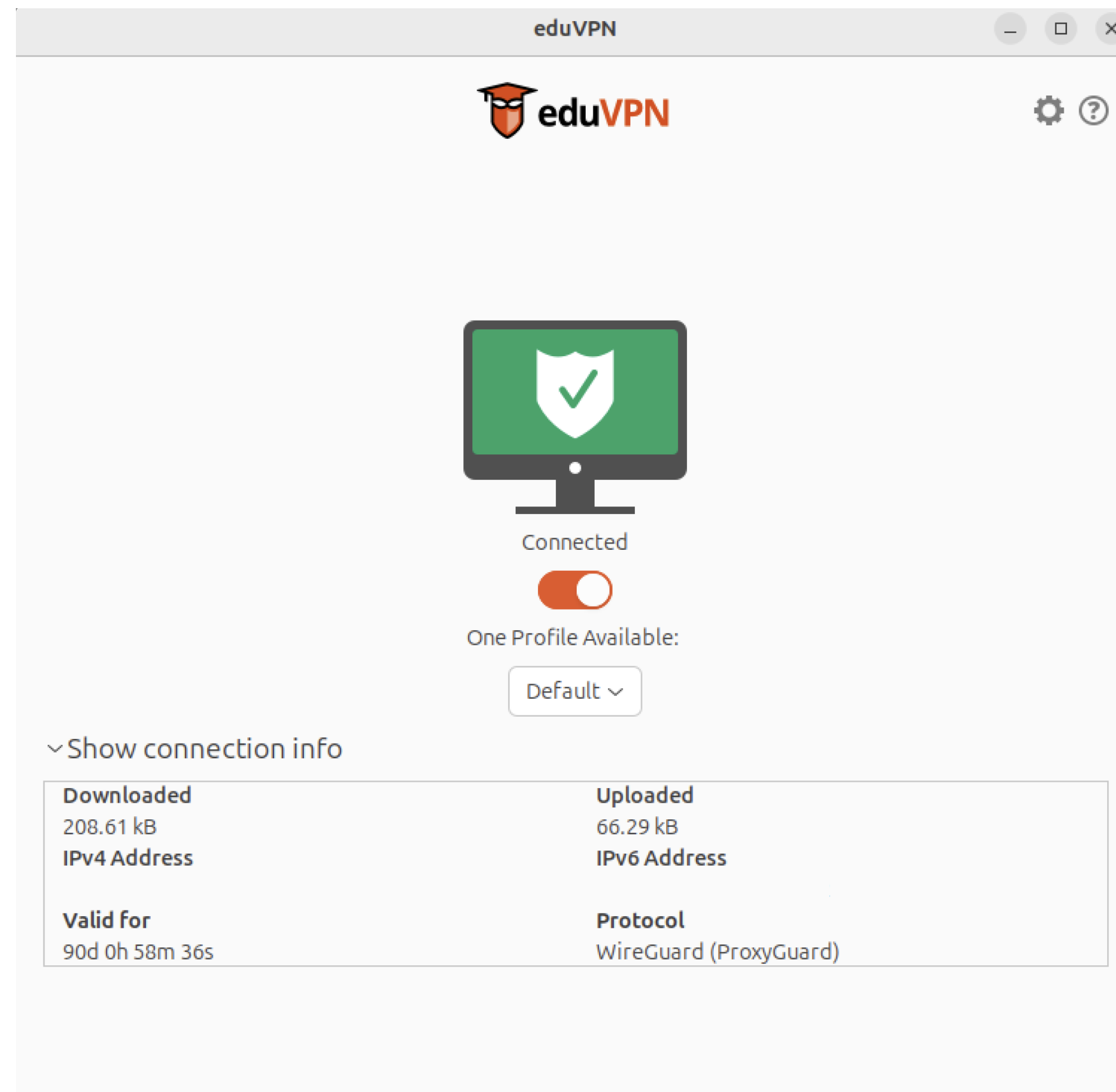
Challenges & Future plans

- Initial impl. easy

- Performance testing and improvements

- Roaming and routing issues 🙁

- Investigate macOS/iOS/Android

- Linux daemon

  - Automatically restart on sleep, roaming

  - Get WireGuard properties dynamically

Questions?

- https://codeberg.org/eduvpn/proxyguard

- Come visit us and our friends

- WireGuard stand:

  - 🏡 Building K, Level 1, stand 6

- NLnet stand:

  - 🏡 Building K, Level 2, stand 13

- GÉANT stand:

  - 🏡 Building F, Level 2, stand 6