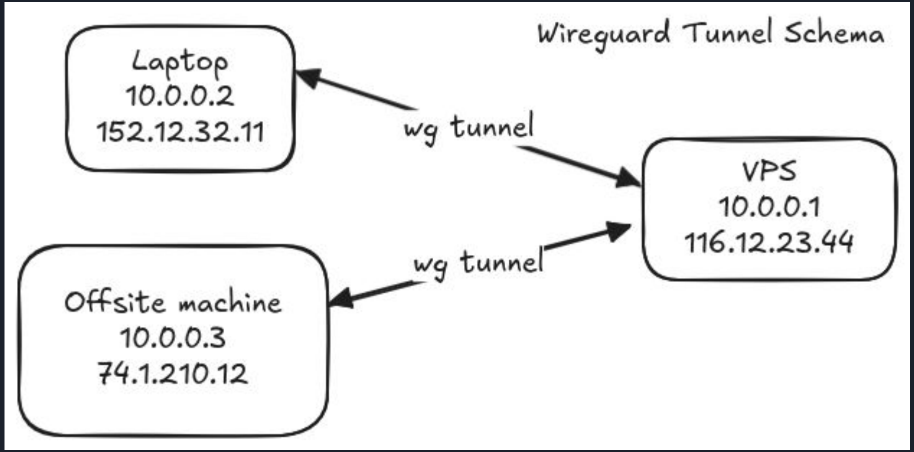
Running your own VPN (RYO VPN)

2025-03-25 Lightning Talk at Leipzig Gophers #49
Martin Czygan

Goal

To connect machines across locations (home, mobile, other, …).

Tailscale (2019) builds on **WireGuard** (2015) to offer **VPN** solutions, and most of the components are open source, e.g. the **tailscale** client.



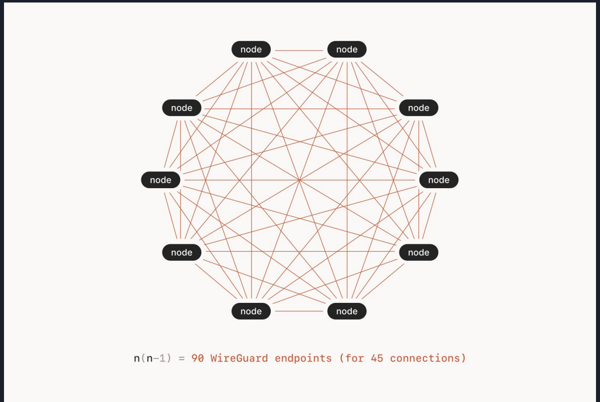
PS. Wireguard is included in **Linux 5.6** (2020)

WireGuard / tailscale

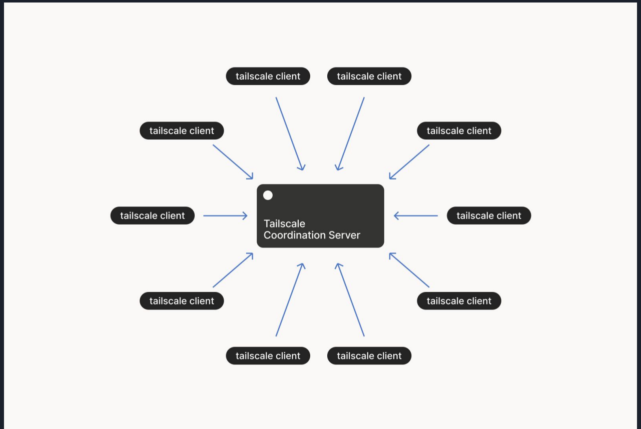
- (mostly) **point-to-point** tunnel exposed as a virtual network device “wg0”
- two endpoints use public-key crypto to setup encrypted connection

Easy, fast secure.

Tailscale adds another management layer on top of wireguard, using a **control server** that manages key exchange, visibility, DNS and more.



n(n−1) = 90 WireGuard endpoints (for 45 connections)

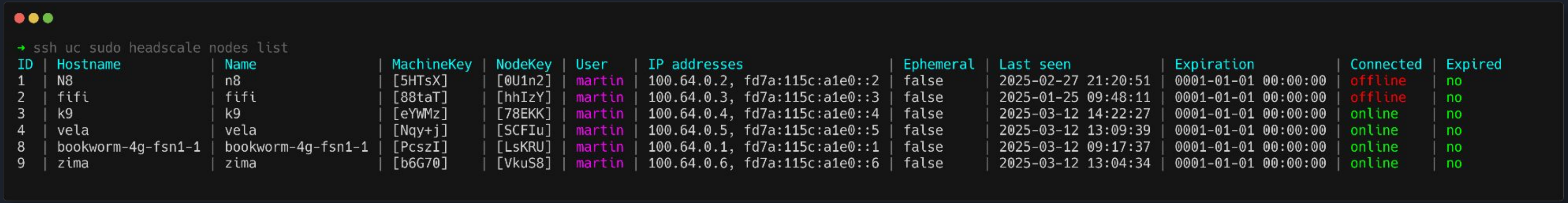


Headscale

- headscale is an open source implementation of the **tailscale control server**

You can run headscale on your own, on a **VPS** for example and have all your machines connected in a single mesh overlay.

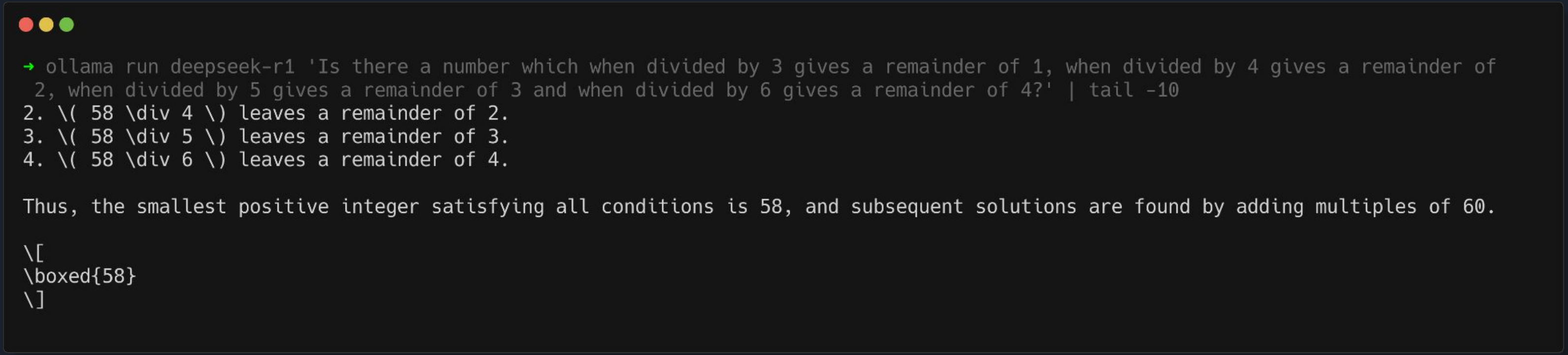
headscale allows a client to “**tailscale login --login-server my.vps**” and then you register the node on the headscale server, and done.



```
➜ ssh uc sudo headscale nodes list
ID | Hostname           | Name               | MachineKey | NodeKey | User   | IP addresses                   | Ephemeral | Last seen           | Expiration          | Connected | Expired
1  | N8                 | n8                 | [5HTsX]    | [0U1n2] | martin | 100.64.0.2, fd7a:115c:a1e0::2 | false     | 2025-02-27 21:20:51 | 0001-01-01 00:00:00 | offline   | no
2  | fifi               | fifi               | [88taT]    | [hhIzY] | martin | 100.64.0.3, fd7a:115c:a1e0::3 | false     | 2025-01-25 09:48:11 | 0001-01-01 00:00:00 | offline   | no
3  | k9                 | k9                 | [eYWMz]    | [78EKK] | martin | 100.64.0.4, fd7a:115c:a1e0::4 | false     | 2025-03-12 14:22:27 | 0001-01-01 00:00:00 | online    | no
4  | vela               | vela               | [Nqy+j]    | [SCFIu] | martin | 100.64.0.5, fd7a:115c:a1e0::5 | false     | 2025-03-12 13:09:39 | 0001-01-01 00:00:00 | online    | no
8  | bookworm-4g-fsn1-1 | bookworm-4g-fsn1-1 | [PcszI]    | [LsKRU] | martin | 100.64.0.1, fd7a:115c:a1e0::1 | false     | 2025-03-12 09:17:37 | 0001-01-01 00:00:00 | online    | no
9  | zima               | zima               | [b6G70]    | [VkuS8] | martin | 100.64.0.6, fd7a:115c:a1e0::6 | false     | 2025-03-12 13:04:34 | 0001-01-01 00:00:00 | online    | no
```

Use cases / limits

- I run ollama (local **LLM** tool) on a desktop machine (behind NAT) and can connect to it from my laptop from anywhere (behind NAT)
- offsite **backup, testing** private projects on **mobile** devices, …
- limits: cannot run multiple tailnets at the same time with headscale



```
➜ ollama run deepseek-r1 'Is there a number which when divided by 3 gives a remainder of 1, when divided by 4 gives a remainder of
 2, when divided by 5 gives a remainder of 3 and when divided by 6 gives a remainder of 4?' | tail -10
2. \( 58 \div 4 \) leaves a remainder of 2.
3. \( 58 \div 5 \) leaves a remainder of 3.
4. \( 58 \div 6 \) leaves a remainder of 4.

Thus, the smallest positive integer satisfying all conditions is 58, and subsequent solutions are found by adding multiples of 60.

\[
\boxed{58}
\]
```

RYO Cloud?

- could you build and run your own cloud provider with a fleet of machines that are part of a tailnet?
- If you are curious, let’s hack together on that!

Thanks!