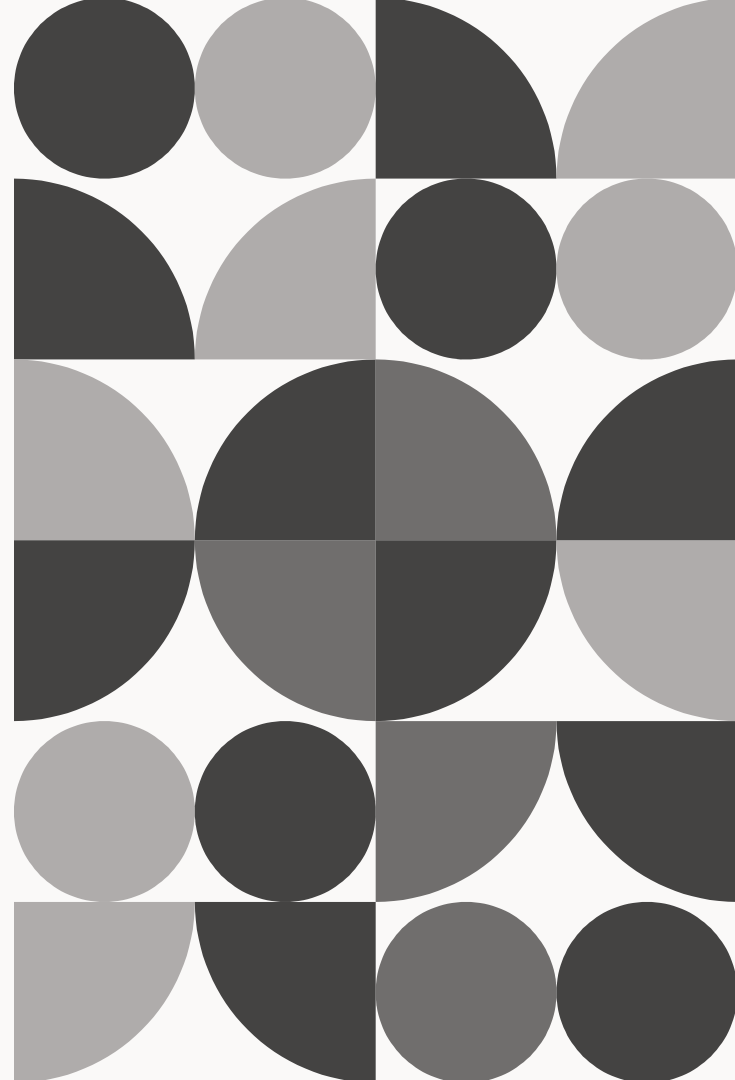


SCALE 23X

Punching Through Firewalls Without Punching Holes

03.08.2026





Not Alex Kretzschmar

Howard



I'm Kevin Purdy, here's how I got here



ANNOUNCEMENTS

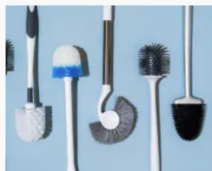
Five Lists of Five Things I Learned at Lifehacker

Today is my last day as the "morning guy" at Lifehacker. I wrote approximately 5,883 posts in slightly less than three and a half years. Some, I hope, were notable. Some make me cringe. I've pulled out a few posts

BY KEVIN PURDY



GET OUR TOP STORIES
FOLLOW LIFEHACKER



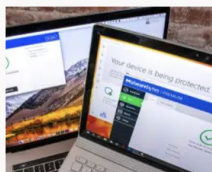
The Best Toilet Brush

Updated January 22, 2026



You Can Build an Ebike. Yes,

Updated June 24, 2022



You Don't Need to Buy Antivirus

Updated April 21, 2020

I RESPECT YOU TECHNICALLY

As the Kernel Turns: Rust in Linux saga reaches the "Linus in all-caps" phase

Torvalds: You can avoid Rust as a C maintainer, but you can't interfere with it.

KEVIN PURDY - FEB 21, 2025 1:55 PM | 224

Lifehacker

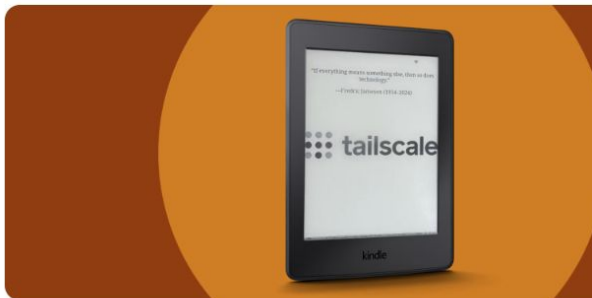
Ask me about blogging before proxy-Hulk-Hogan took it down

Wirecutter

Ask me about mattresses. Or recycled toilet paper. Or cutting boards.

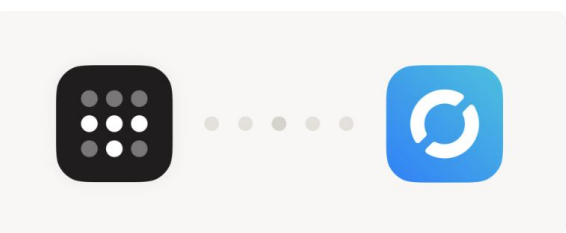
Ars Technica

Ask me about ... the Linux Kernel Mailing List?



Insights December 01, 2025

Let's put Tailscale on a jailbroken Kindle



```
• stirling
tag:container
Expiry disabled Ephemeral

• bazzite
somebody@tailscale.com
Expiry disabled

• printer
somebody@tailscale.com
Expiry disabled SSH

• purdeck
somebody@tailscale.com
Expiry disabled SSH

• chromebook2
somebody@tailscale.com
```

```
Tailscale - SSH to printer
about:blank
Linux raspberrypi 6.6.51+rpt-rpi-v7 #1 SMP Raspbian 1:6.6.51+rpt
3 (2024-10-08) armv7l

The programs included with the Debian GNU/Linux system are free so
ftware;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Wed Jul 30 16:53:20 EDT 2025 from 100.72.57.3 on pts/0
kevinpurdy@raspberrypi:~$
```



Insights September 22, 2025

Upgrade your travel kit with a tiny, Tailscale-friendly router

I'll be on vacation when this post is published. It's not a tropical, cultural, or adventure vacation, but a kind of remote staycation, in a big rented house, with...

 Kevin Purdy

And now I do this!

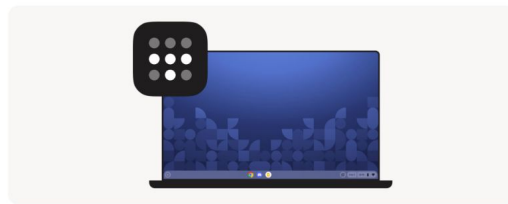


Insights November 04, 2025

Why you should mail your parents a Tailscale node

Set up a VPN, remote tech support, file sharing, and other useful things by mailing a little Tailscale to your friends and family.

 Kevin Purdy



Homelab

Education! Refurbishment! Unpaid labor! Backups of ... your Linux ISOs, yes.



But really, anything is a homelab

(Except an iPad)




- Raspberry Pi
- Mac mini
- NUC from a dentist's office
- Laptop w/ or w/o screen

Warning: Self-hosting is addictive

June 2, 2025:
0 Containers

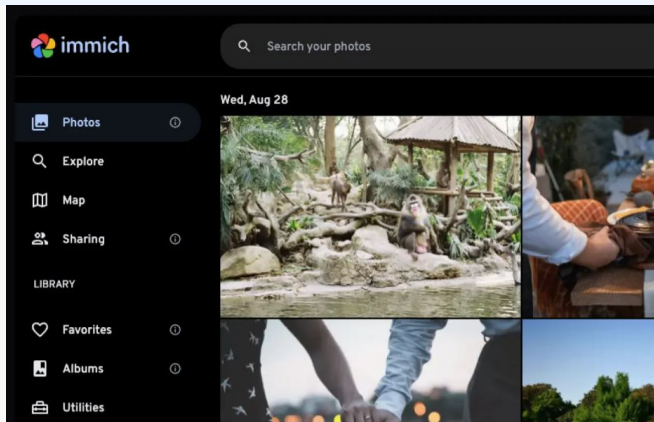
March 4, 2026:
33 Containers



DumbWare
We believe in the power of stupid simple solutions.
Verified



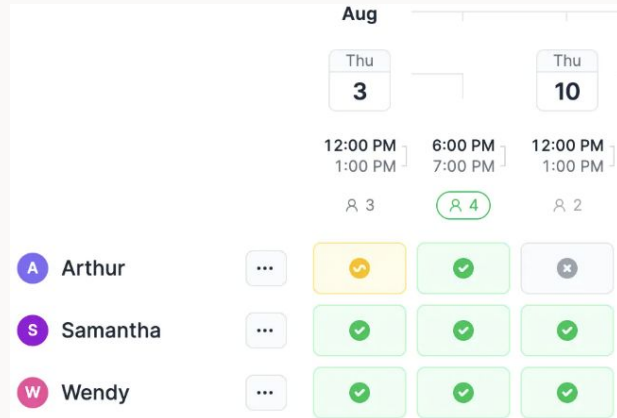
FreshRSS



immich Search your photos

Wed, Aug 28

- Photos
- Explore
- Map
- Sharing
- LIBRARY
- Favorites
- Albums
- Utilities



Aug

Thu 3	Thu 10	
12:00 PM - 1:00 PM	6:00 PM - 7:00 PM	12:00 PM - 1:00 PM
3	4	2
Arthur	✓	✗
Samantha	✓	✓
Wendy	✓	✓

**Your PDFs.
Your Control.**

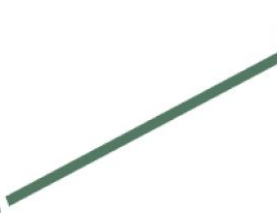
The world's most secure PDF platform.
AI-native and completely private.

I thought this talk was about firewalls
and ports?



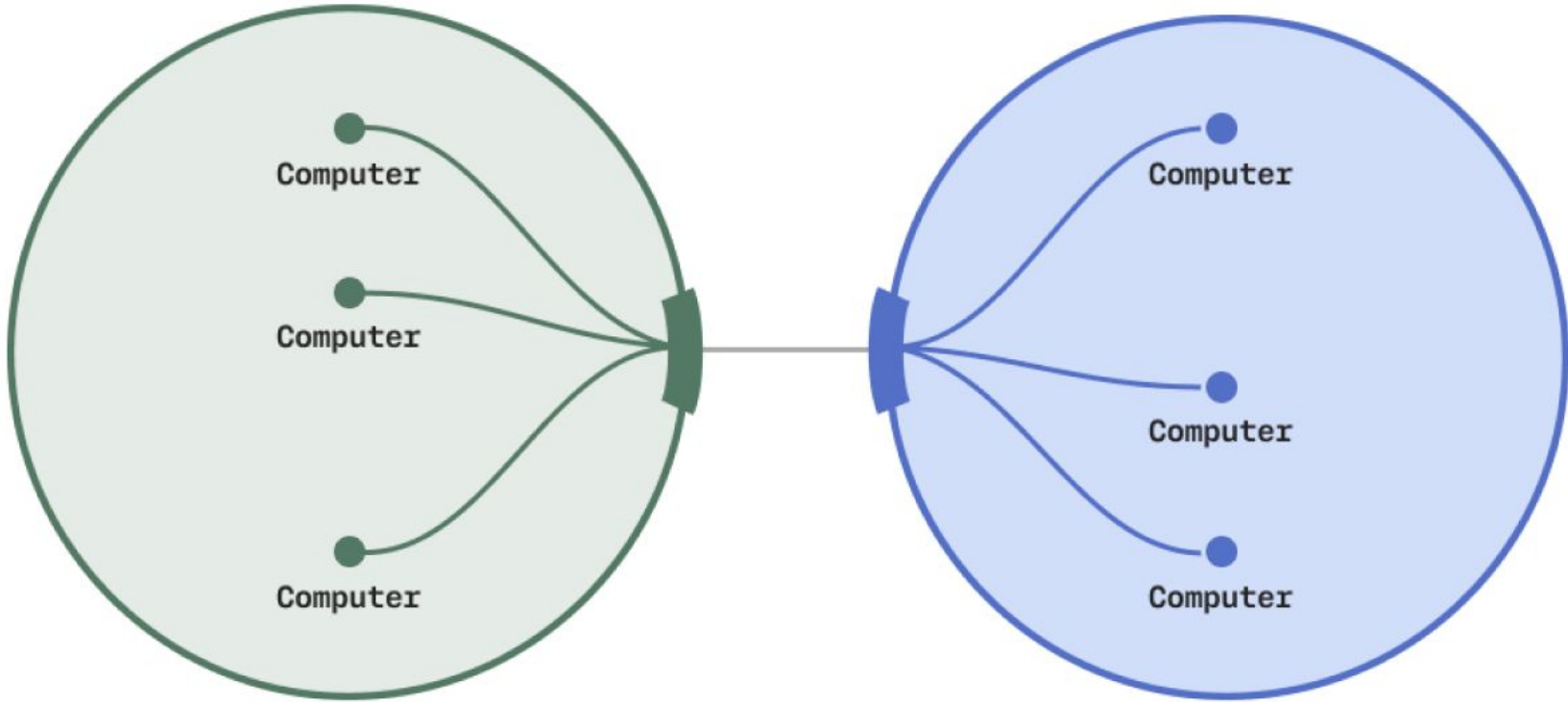
Computer

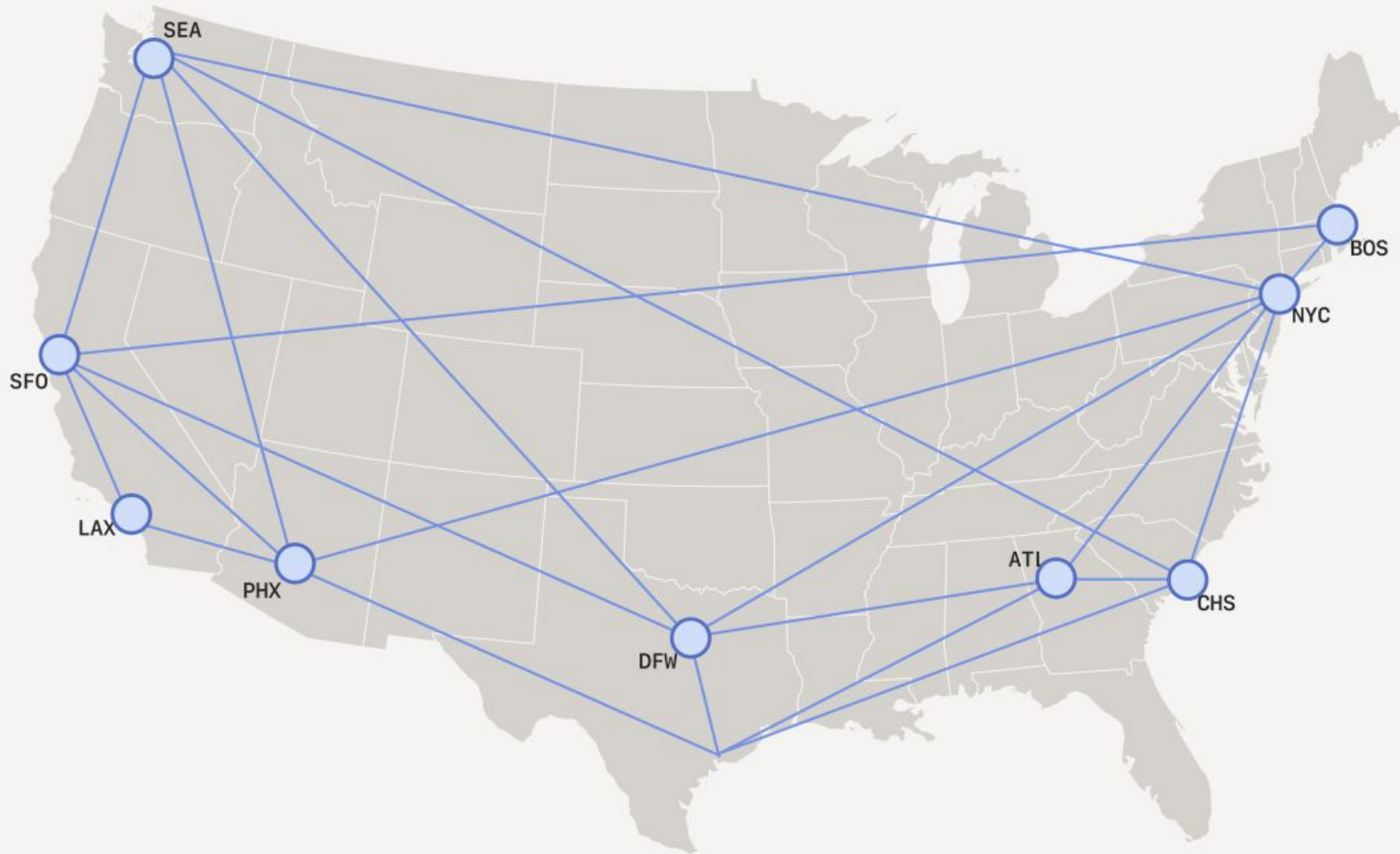
Computer

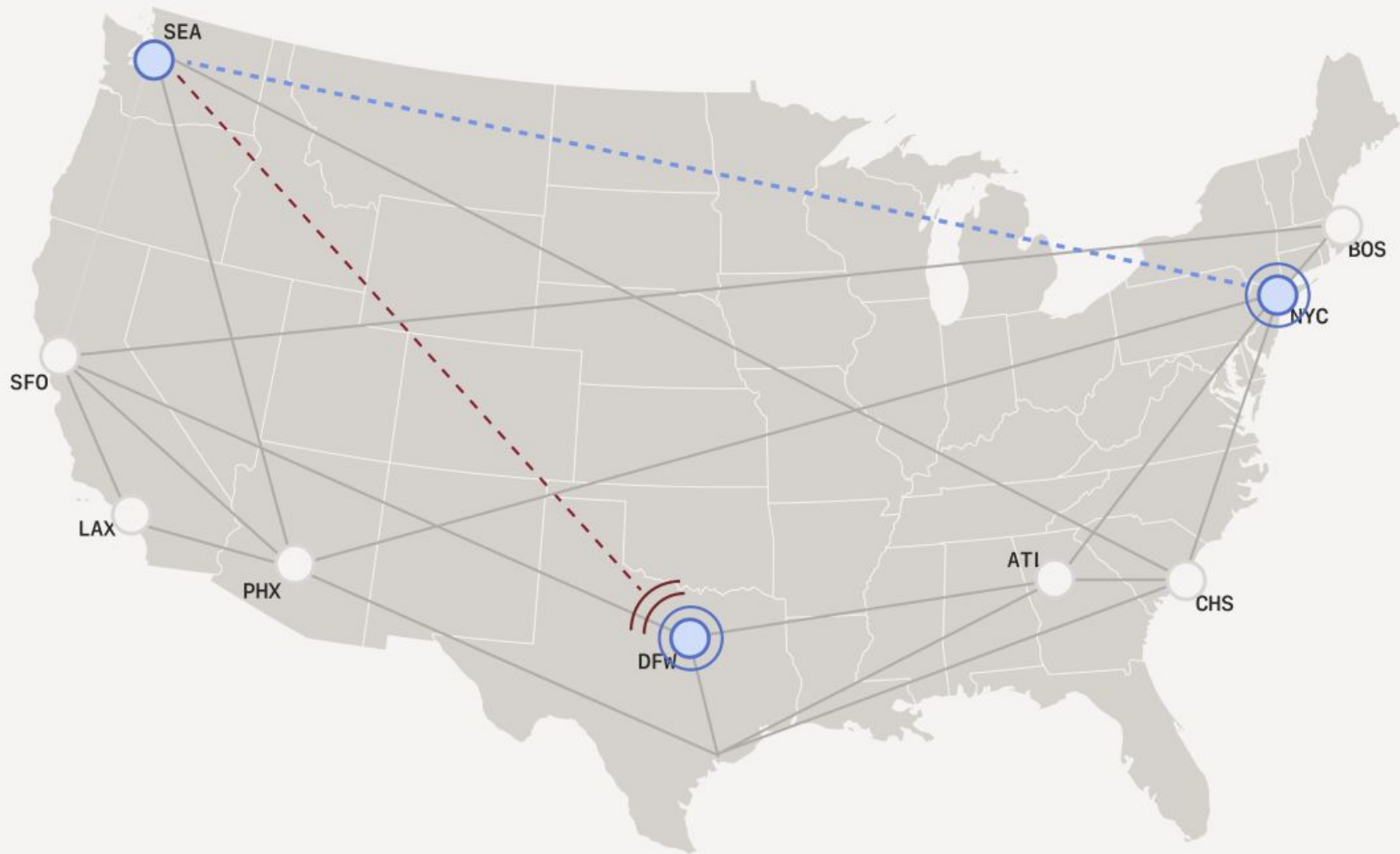


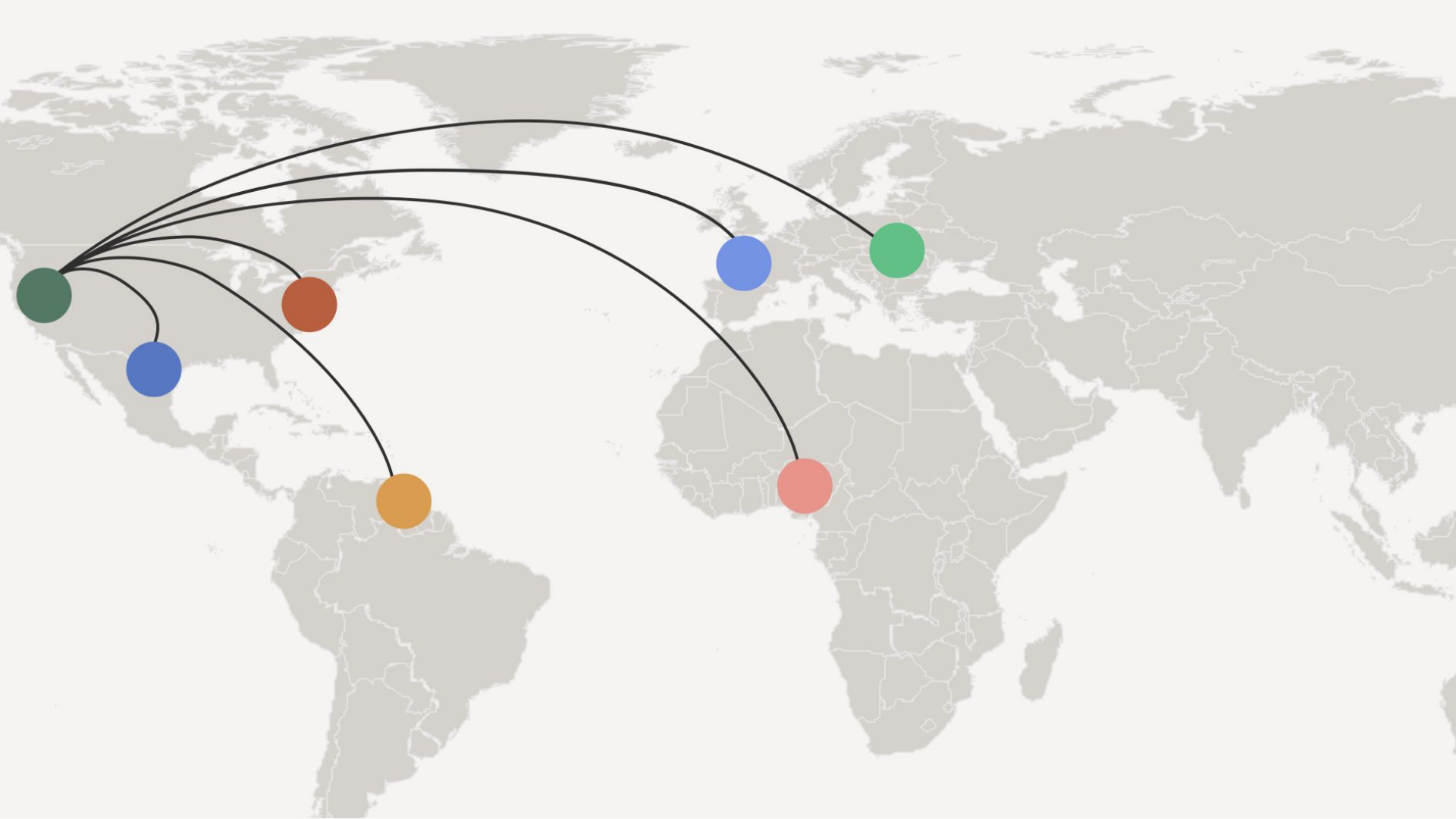
Computer

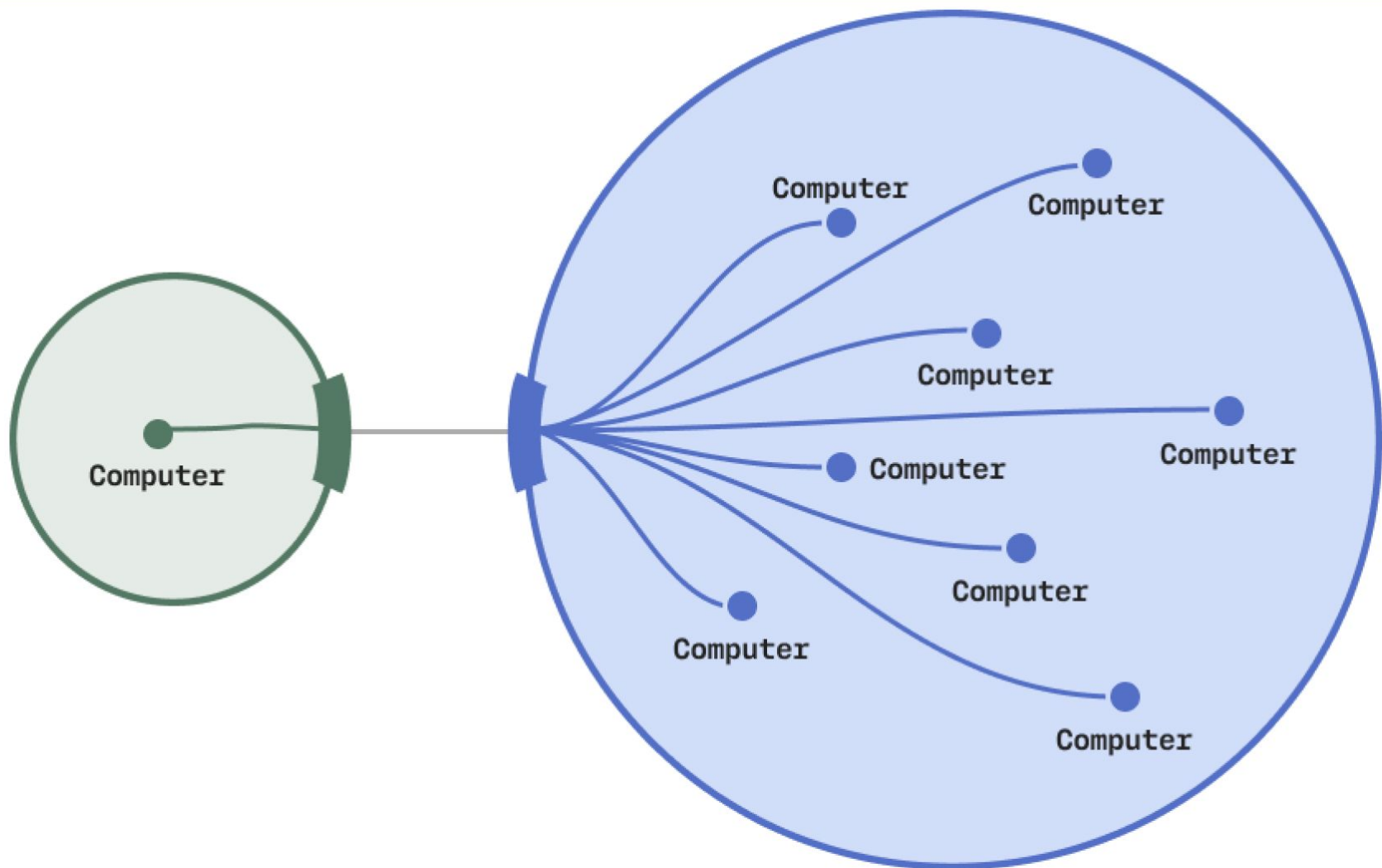
Computer





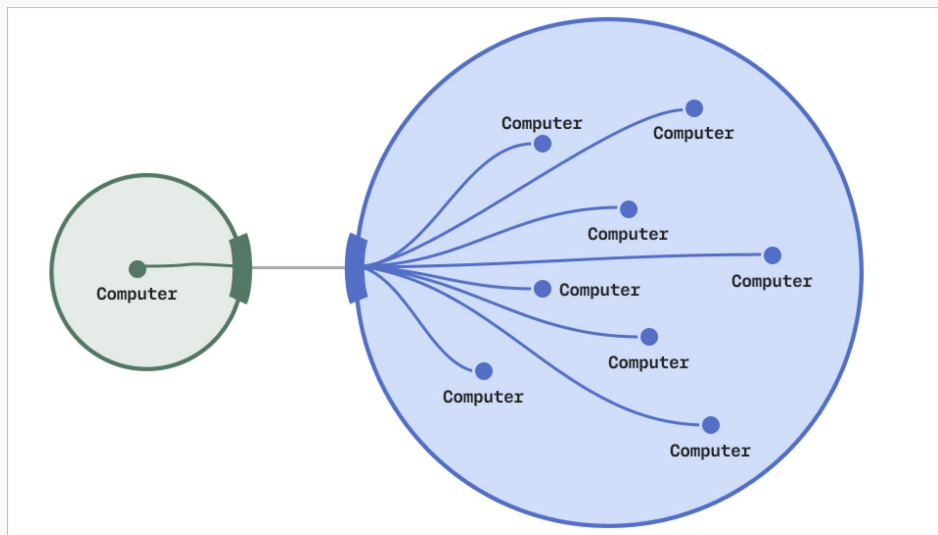


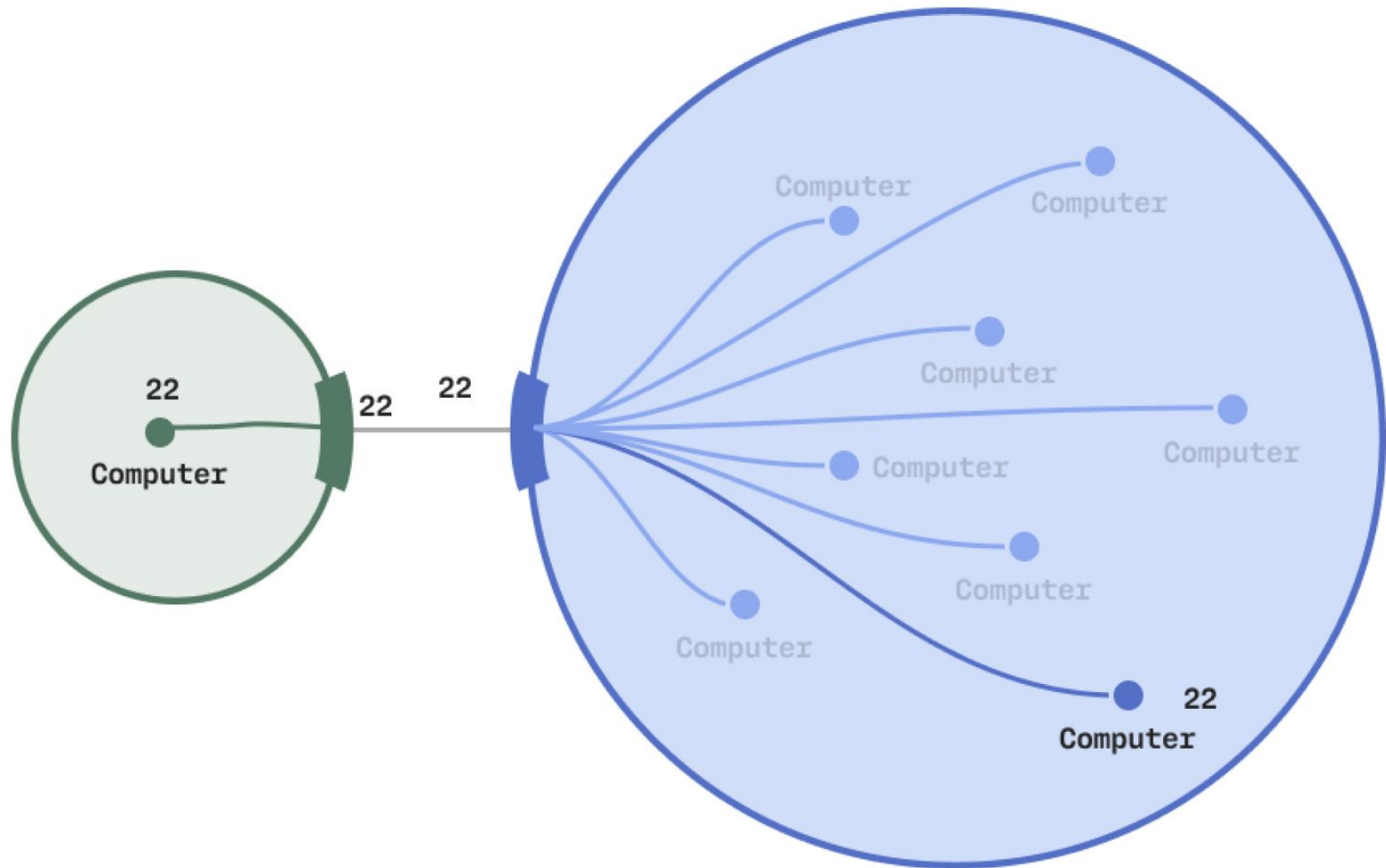




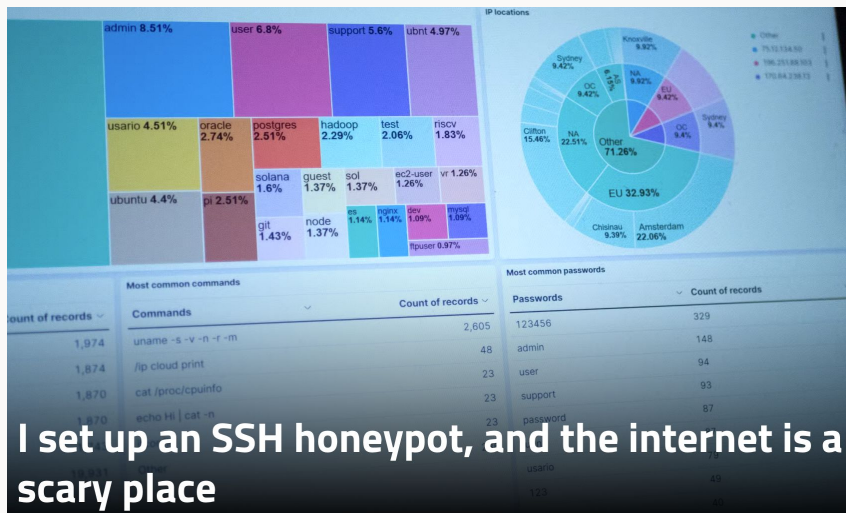
Network Address Translation (NAT)

Allows multiple devices on a private network to share a single public IP when accessing the internet.





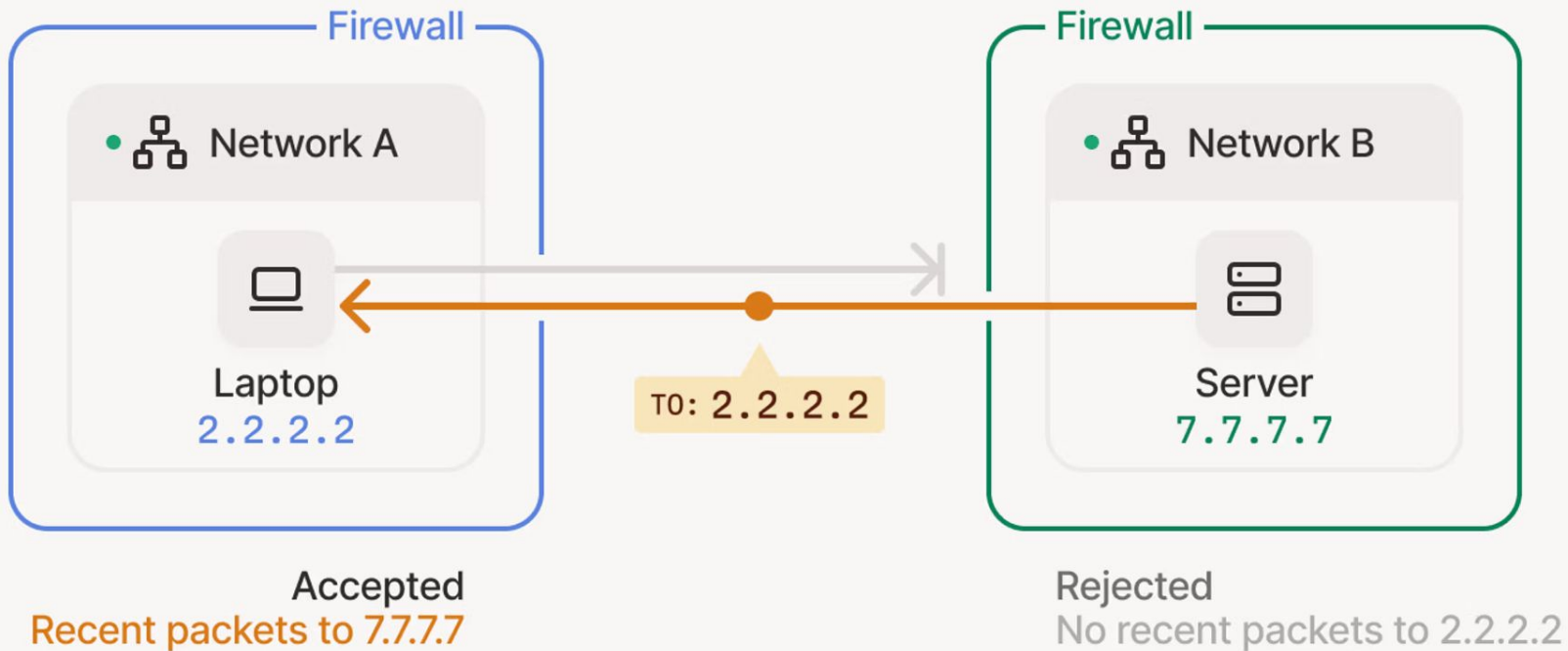
Why don't we just forward ports?



- 29,282 unique interactions
- 447 unique IP addresses
- NoaBot, IRC worms, Telegram grabs



NATs, firewalls: Now what?



/me reaches into bag of tricks

STUN

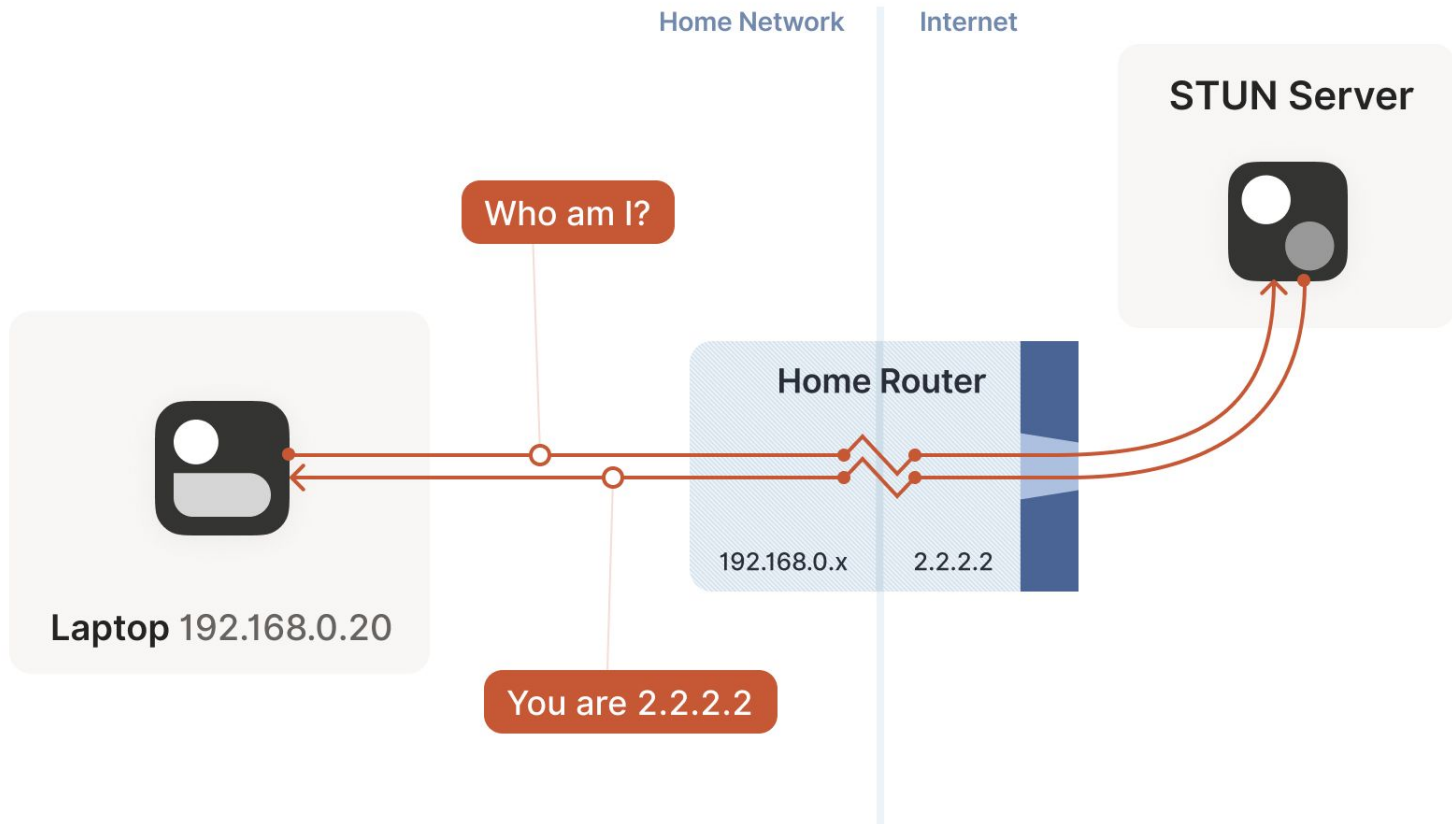
What actual address
did these packets
come from?

192.168.1.50:12345

>>>

203.0.113.7:45123

"Here's the address your packets
actually came from"



UDP hole-punching

Let's show these firewalls we're good friends

Coordination server
has both sides send
packets at the same
time

Each firewall sees:

```
203.0.113.7:45123 → 192.168.1.42:41641  
192.168.1.42:41641 → 203.0.113.7:45123
```

Let the packets flow!

Nothing says the packets must
be related to each other!

Symmetric ("Hard") NAT

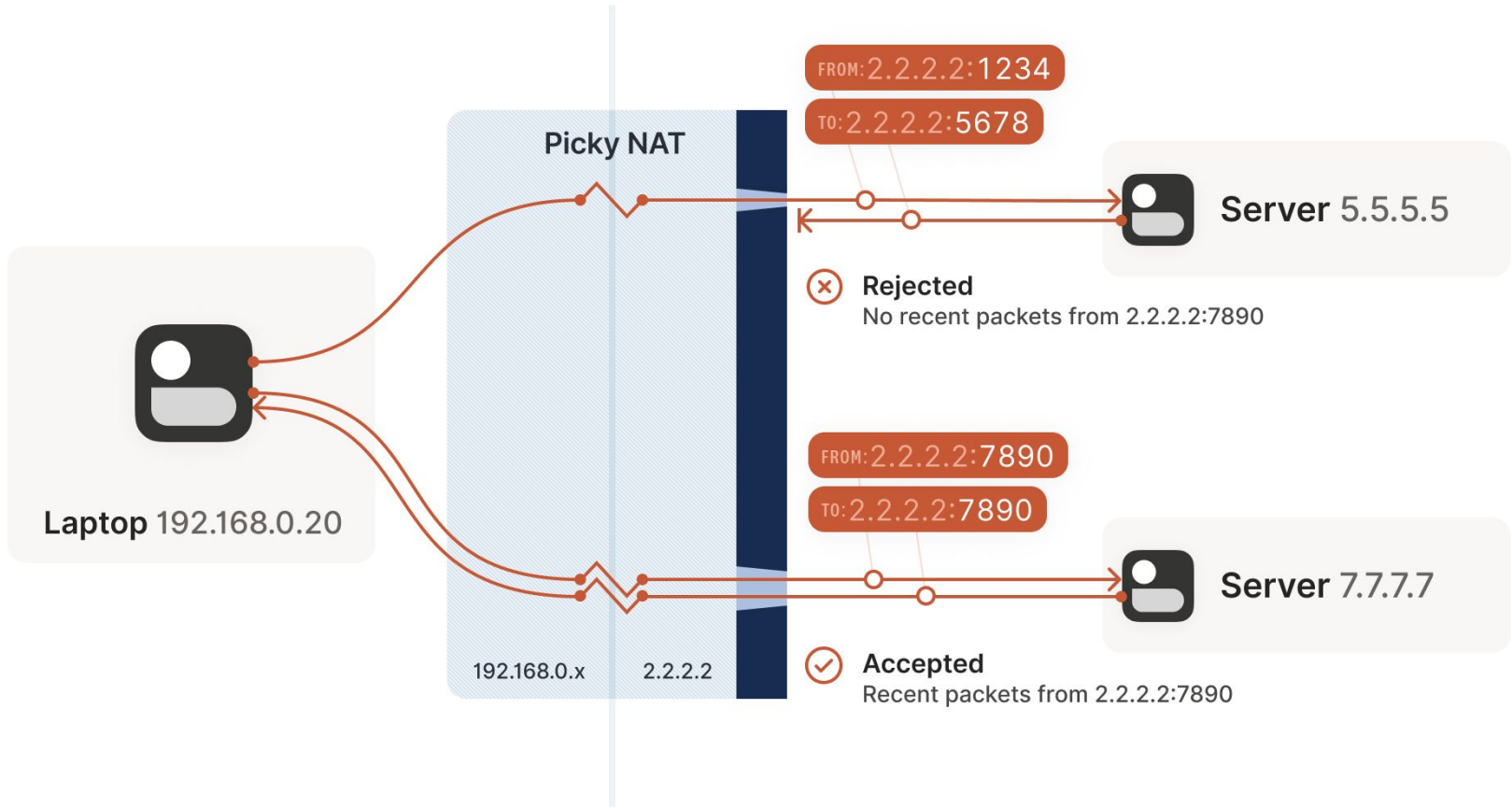
Randomize the port
for every outgoing
connection

192.68.1.42 wants to go to
7.7.7.7:

"You are 2.2.2.2:1234"

192.168.1.42 wants to go to
8.8.8.8:

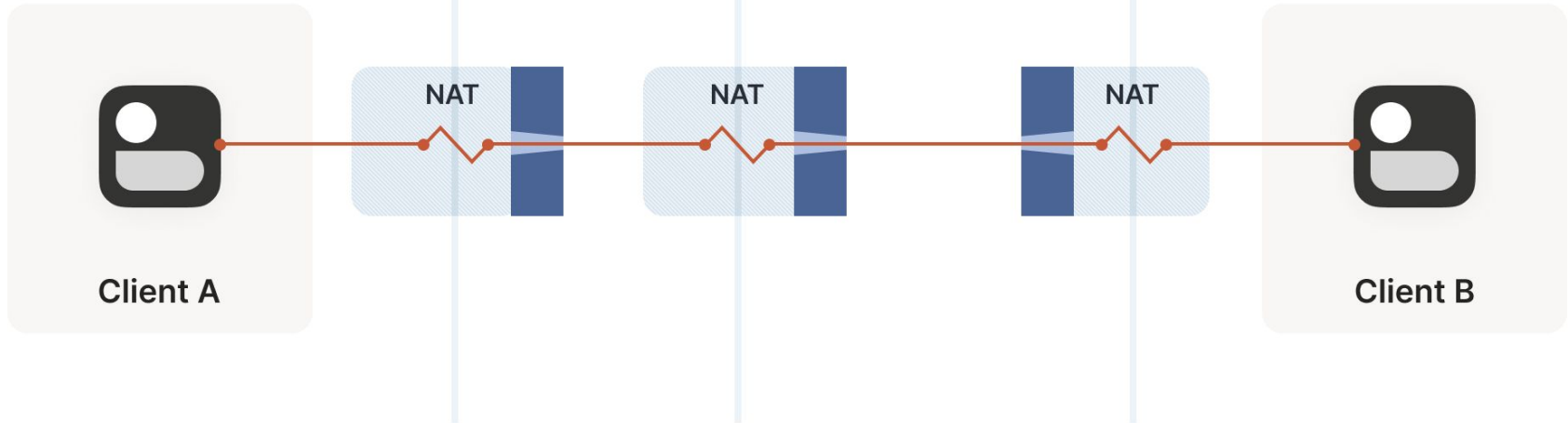
"You are 2.2.2.2:6789"



Home Network

ISP Network

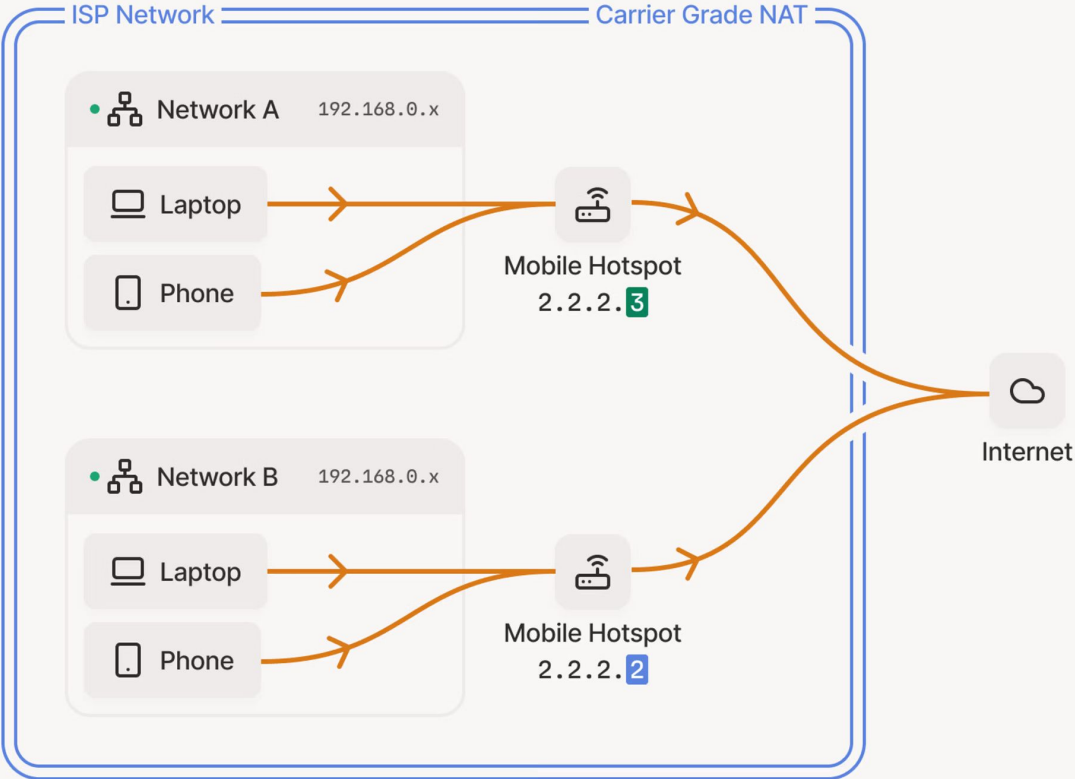
Office Network

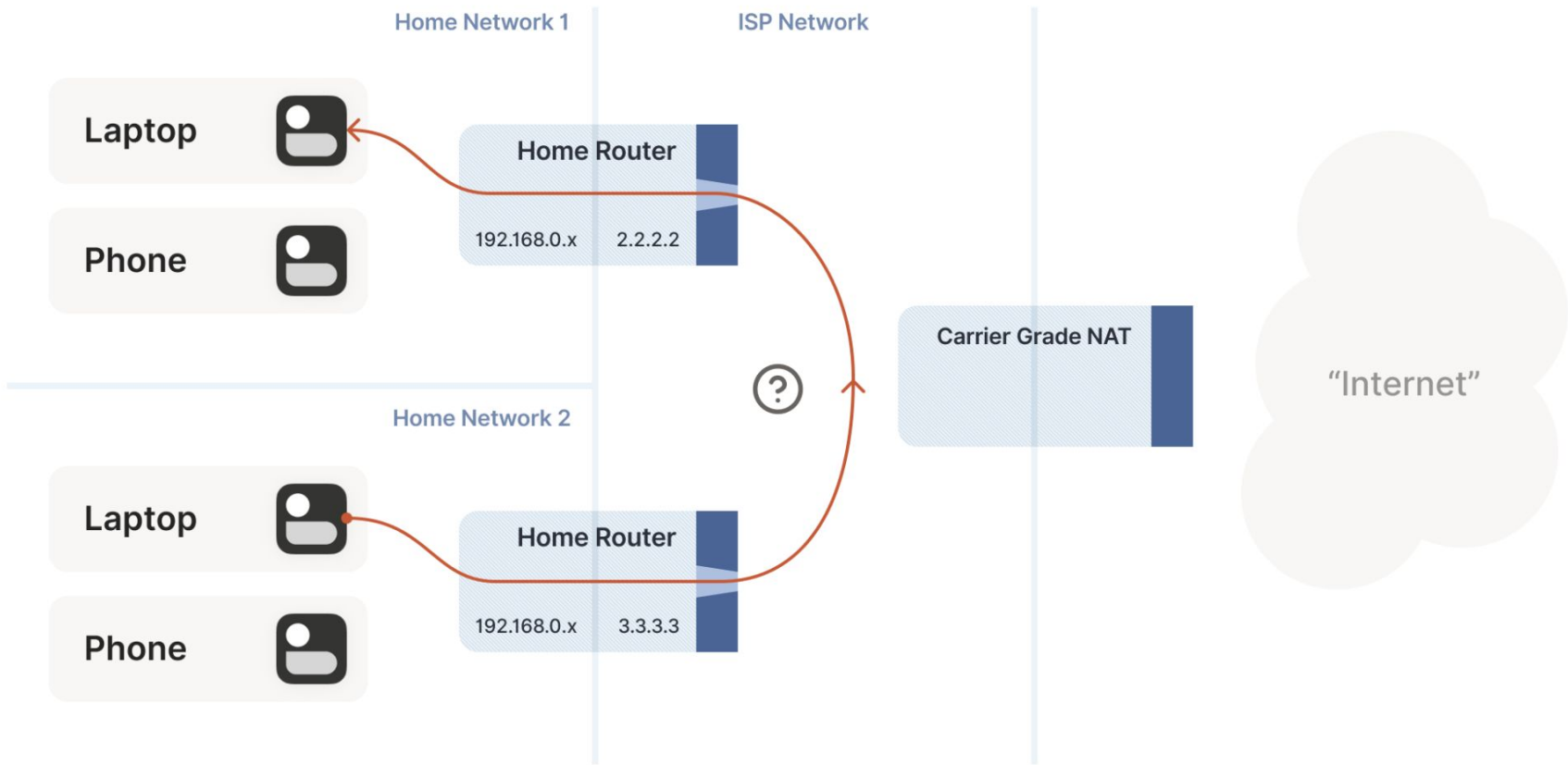


Client A

Client B

Carrier-





Deeper in the bag of tricks

The “Birthday Paradox”

Number of random probes	Chance of success
174	50%
256	64%
1024	98%
2048	99.9%

The “Halo and Zoom” Set

- UPnP
 - A whole bunch of late 90’s tech to temporarily forward ports
- NAT-PMP (v2) / PCP
 - A sane, reduced NAT traversal tool

Side channels

- “Let’s talk in private about our ports”

ICE: Let's try everything! (responsibly)

- IPv6
- IPv4 LAN ports (local)
- IPv4 WAN (STUN)
- IPv4 WAN mapped by protocol
- Static port-forwards

Open a side channel, check both sides' options, send some UDP, and see what works best

And then there were Relays

Like humans, some networks aren't complicated, they're just jerks

- Enterprise firewalls
- Symmetric NAT
- Carrier-grade NAT
- Carrier-grade NAT that explicitly disallows "hairpinning"
- Hotel/conference Wi-Fi
- Blocking UDP entirely
- Cloud gateways (AWS, Azure, the mean GCS)

NAT traversal is basically optimistic packet spam combined with careful observation of which packets make it through.

(I call it “Genially FA and
Responsibly FO”)

Other "tricks"



freeBSD[®] The Power To Serve

Home

About

Get FreeBSD

Documentation

Community

- » [About](#)
- » [Features](#)
- » [Applications](#)
- » [Administration](#)
- » [News](#)
- » [Events](#)
- » [Press](#)
- » [Artwork](#)

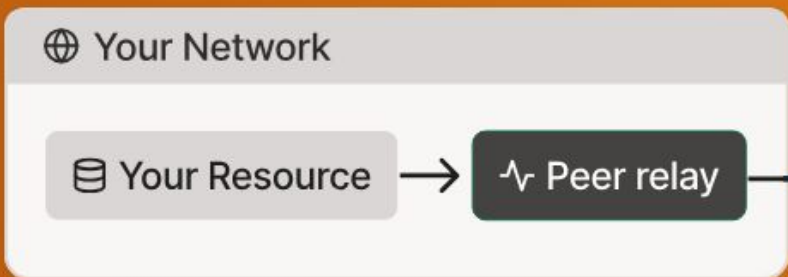
Endpoint-Independent NAT

Contact: Tom Jones <thj@freebsd.org>

This project aims to add support for Endpo

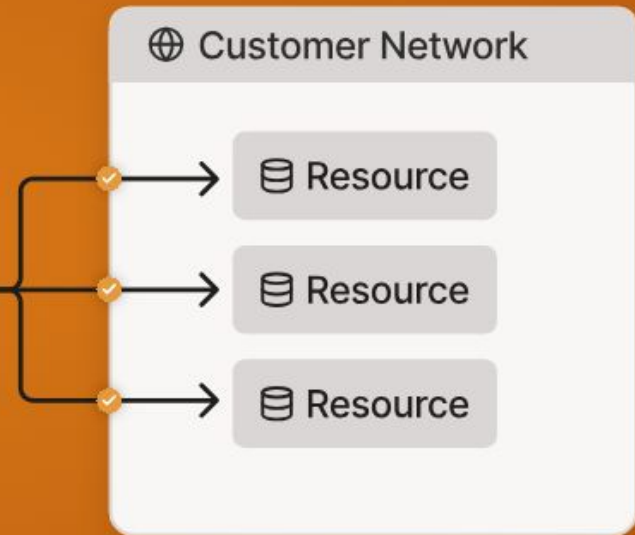
End Point Independent NAT enables applic
application without any NAT traversal me
NAT is transparent and it is as-if there is no
known as 'full-cone' NAT.

Have a pandemic!



Peer relay
ip:port exception

Network Firewall









18
Stacks



33
Containers

 29 running  3 stopped
 0 healthy  0 unhealthy



54
Images

 27.9 GB



11
Volumes



24
Networks



Alright, your turn

 tailscale