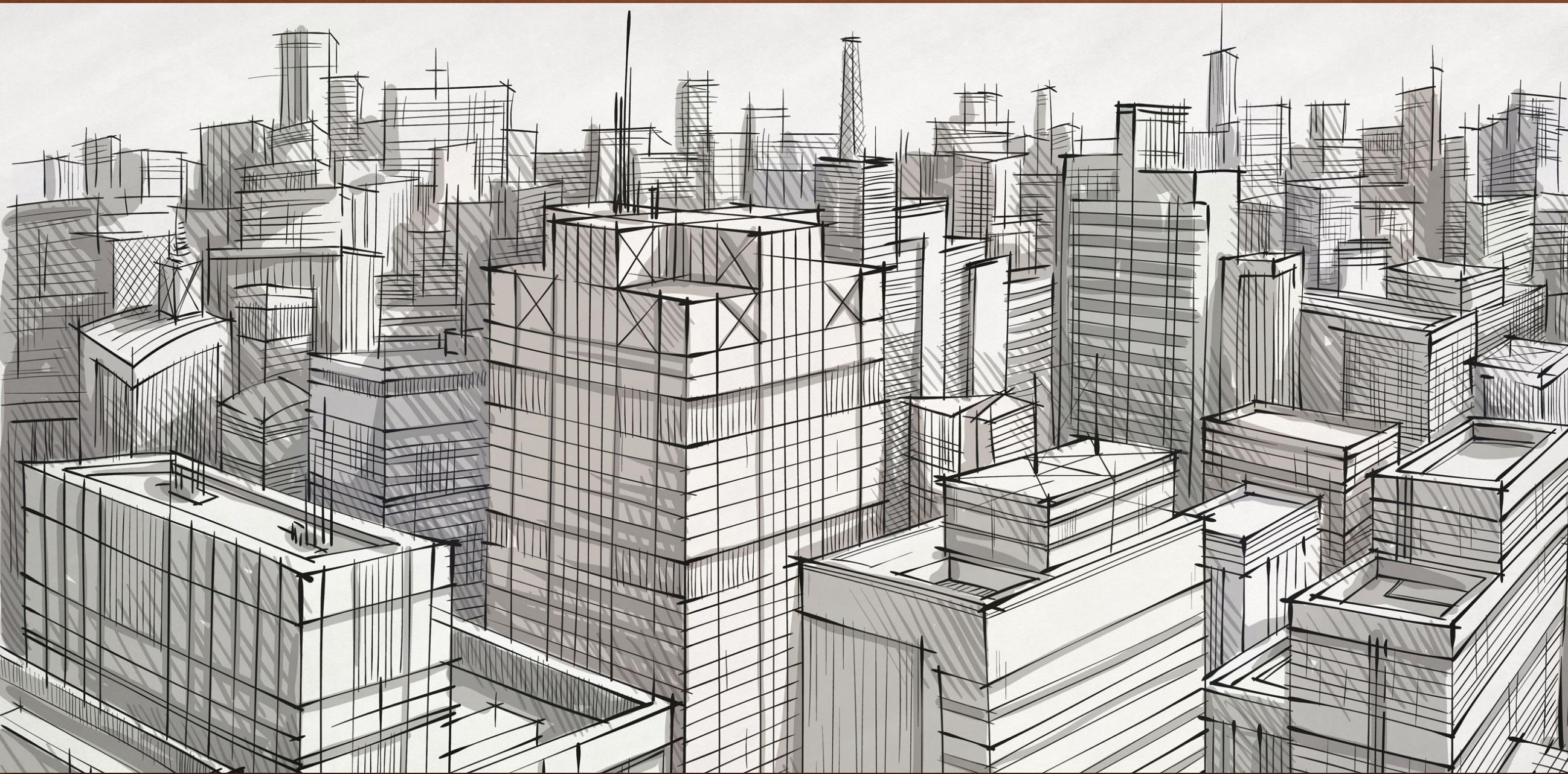


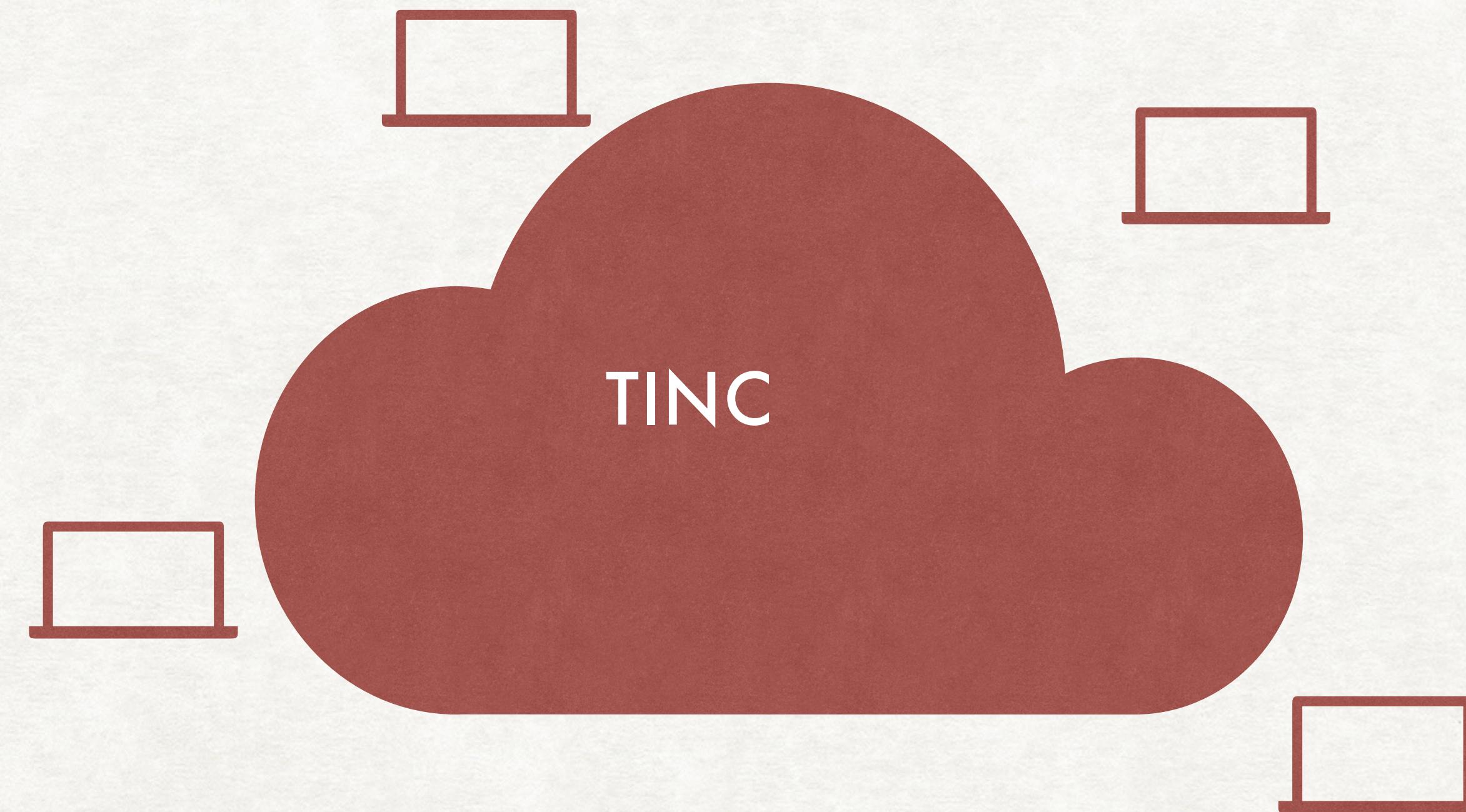
LORENZ KIEFNER  
MESH-VPN  
SELBSTGEBAUT

VPN. CLIENT-SERVER. P2P. MESH.

# WAS IST EIN MESH-VPN?

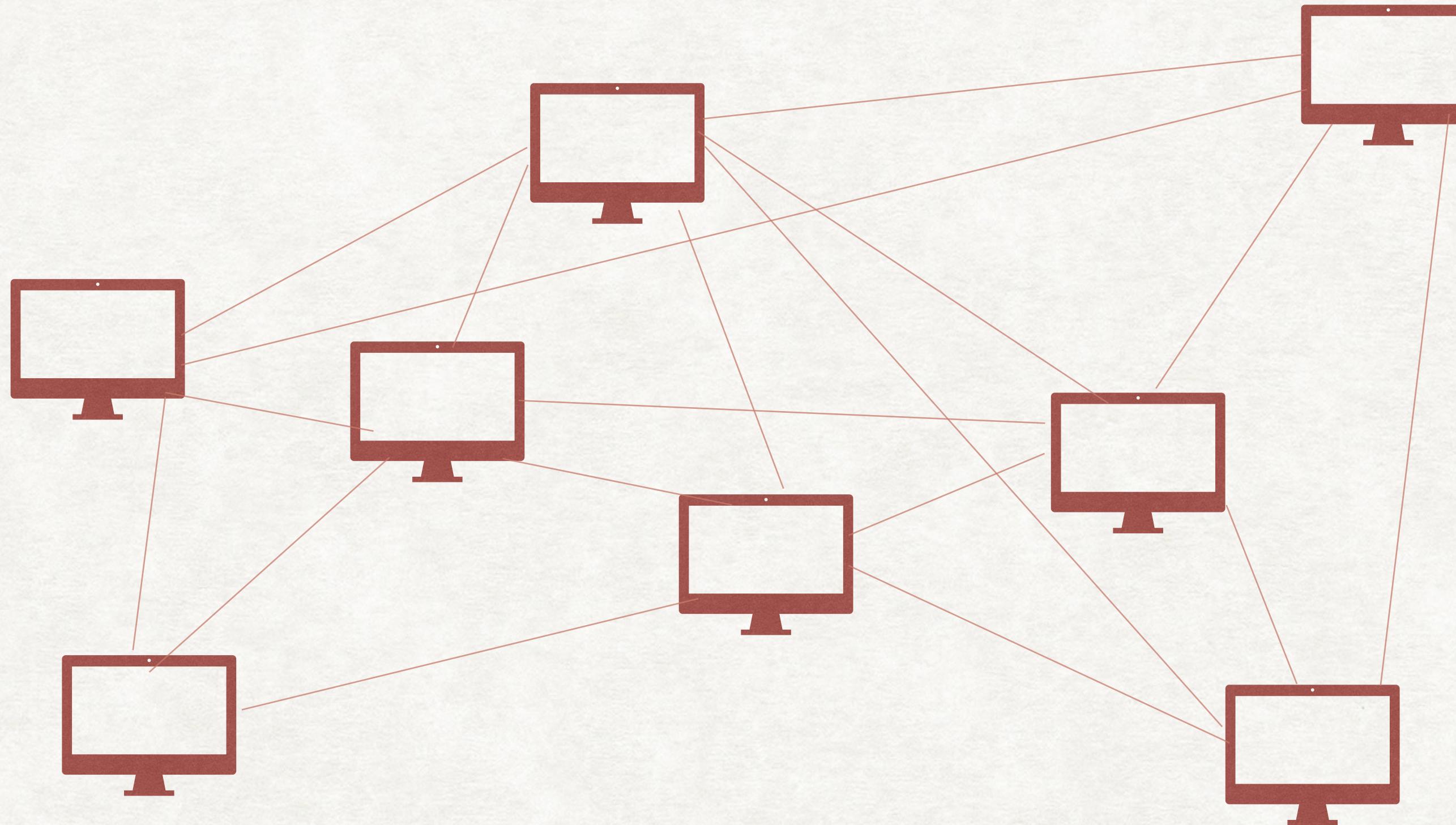


TINC  
„THERE IS NO CABAL“ - [HTTPS://WWW.TINC-VPN.ORG](https://www.tinc-vpn.org)



# MODULARES MESH-VPN

P2P-VPN + ROUTING = MESH-VPN



## IPV6 IST PFLICHT SONST KOMMT ES ZU ADRESSKOLLISIONEN

- Wer verwendet 192.168.178.0/24 im Heimnetz?
- Wer verwendet 192.168.0.0/24 oder 192.168.1.0/24?
- Wer verwendet ein 10er-Netz?
- Der Adressraum des VPNs muss sich von allen anderen Adressräumen unterscheiden, sonst ist kein Routing möglich
- Lösung: Unique Local IPv6-Adressen: fd00::/8
  - Z.B. fd74:fc42:6978::/48

## ROUTING: OSPF MIT BIRD

„BIRD INTERNET ROUTING DAEMON“

- OSPF in Version 3 unterstützt IPv6
- OSPF benötigt Link-Local Adressen
- bird (<https://bird.network.cz>) wird von den meisten europäischen Internet-Knoten verwendet, darunter DE-CIX, AMS-IX

## P2P-VPN GANZ UNTEN...

- Wir brauchen:
  - Link-Local-Adressen für alle Tunnel-Endpunkte
  - Forwarding beliebiger Pakete
  - „Kosten“ eines Tunnels, z.B. basierend auf der Leitungsgeschwindigkeit
- Lieblings-VPN-Lösung (wireguard) lässt nur festgelegte IP-Adressen als Quelle zu? Tunnel darüber!
- GRE (Generic Routing Encapsulation) bietet keine Verschlüsselung, aber die haben wir ja schon
- Achtung: Transport-VPN braucht dann einen eigenen Adressraum, der sich vom Mesh-VPN unterscheidet (z.B. ein weiteres Unique Local Prefix, z.B. fdde:ad74:fc42::/48)

## DAS ZUSAMMENSPIEL UND SO WIRD EIN MESH DARAUS...

- Die gewünschte IP-Adresse, z.B. fd74:fc42:6978:cafe::1/64, bekommt das Loopback-Interface (zusätzlich)
- `sysctl net.ipv6.conf.all.forwarding=1`
- `bird` ermittelt optimale Routen und setzt sie
- Bei Ausfall eines Nodes steht innerhalb der konfigurierten OSPF-Hello-Zeit die dann optimale Route

## STOLPERFALLEN

### ES GIBT IMMER WAS ZU TUN...

- ICMP-Messages aus der Transportebene erreicht keine andere Ebene
- MTU muss klein genug sein, sonst gibt es ICMPv6 „Packet too big“ auf Transportebene, das Paket wird verworfen
- bird muss im gesamten Netz konsistent konfiguriert sein
  - MTU darf nicht asymmetrisch sein
  - OSPF-Hello-Zeit muss übereinstimmen

HAPPY  
TUNNELING!