Starlink, AREDN, and Networking

Tom McDermott, N5EG

September 17, 2022

TAPR / ARRL DCC

Charlotte, North Carolina

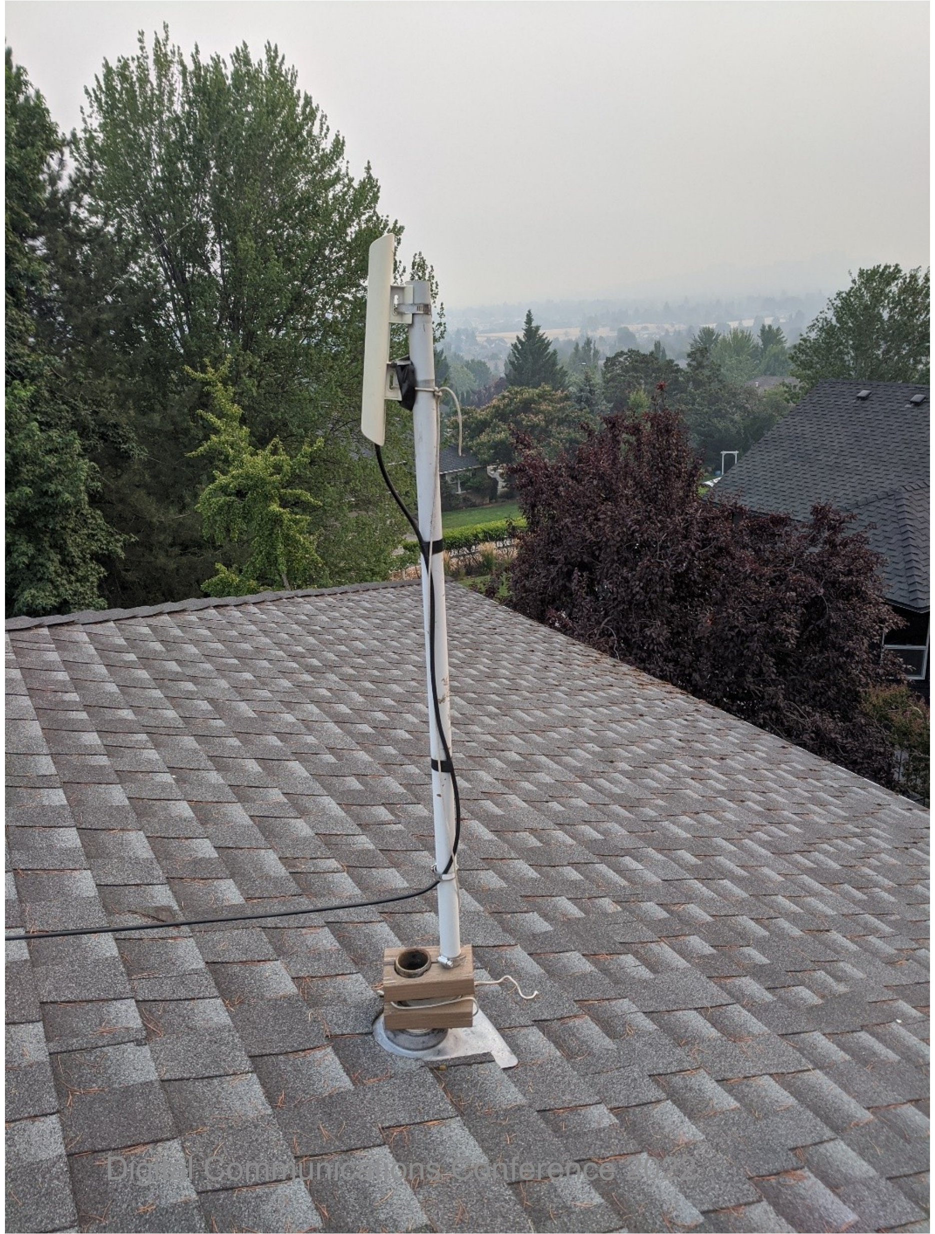
Outline

- AREDN
  - Tunnels, Clients, and Servers
- Starlink
  - How it works
  - Some issues
- Tailscale
  - Free VPN – easy to setup.
- Cloud host
  - Linode, Digital Ocean, Vultr, etc.

AREDN

- Outstanding software for a range of commercially available wireless nodes.
  - Repurposes growing collection of 802.11 WiFi equipment into the Amateur band.
  - Provides Mesh networking. Good link speeds possible.
  - Provides on-board services, routing.
  - Available for 2.4 GHz and 5 GHz amateur bands – dependent on the radios available. 3.3 GHz withdrawn in USA by FCC action.
- Provides support for Internet tunnels.
  - Useful when the distance to a node is too far for RF paths, requires too many hops, the path is obstructed, etc.
    - Tunnel client attempts connection to Tunnel server on another node.
- What to do when Internet is not readily available at the node?

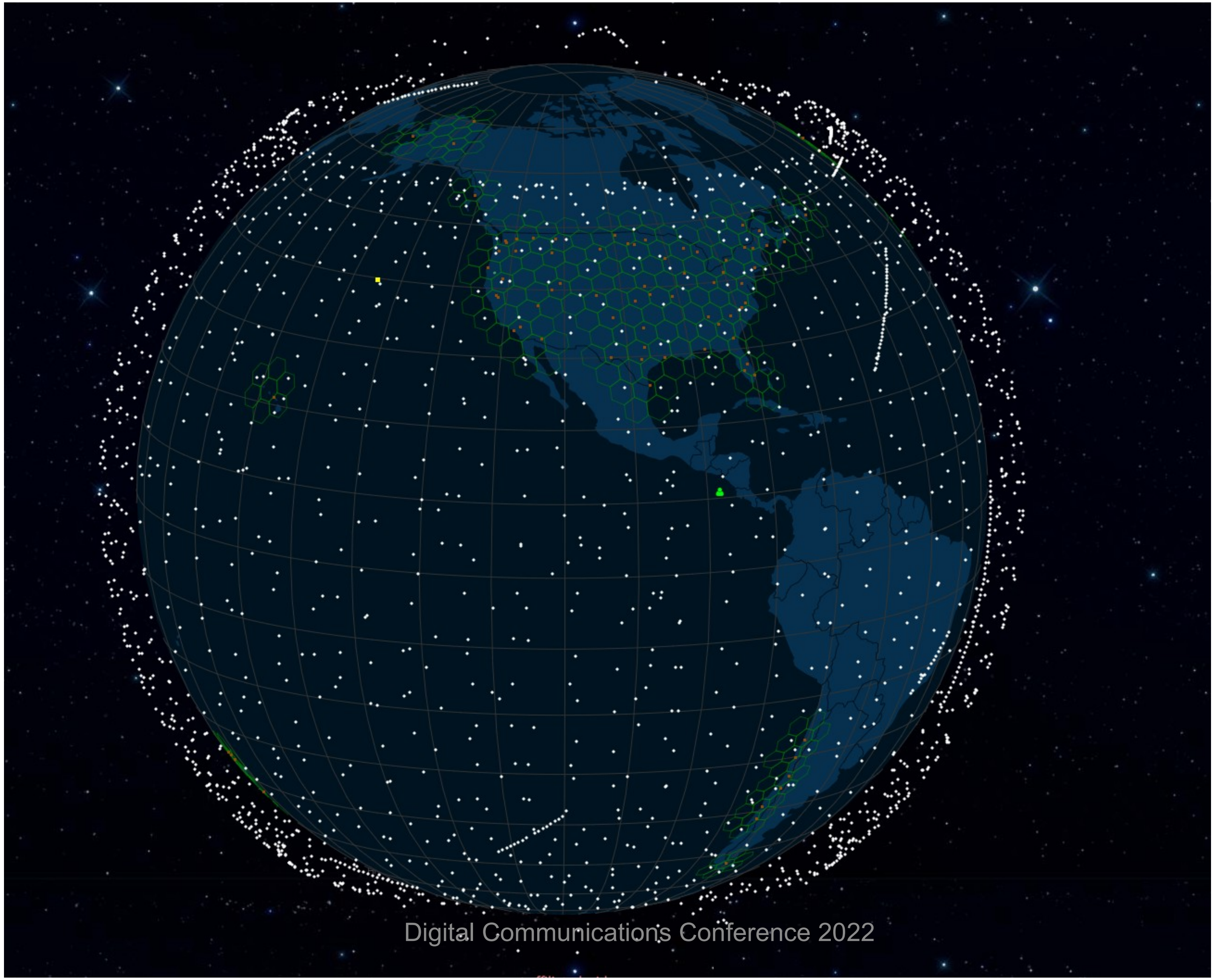
AREDN Node pointed at Mt. Baldy (~10 degrees uptilt)



Starlink

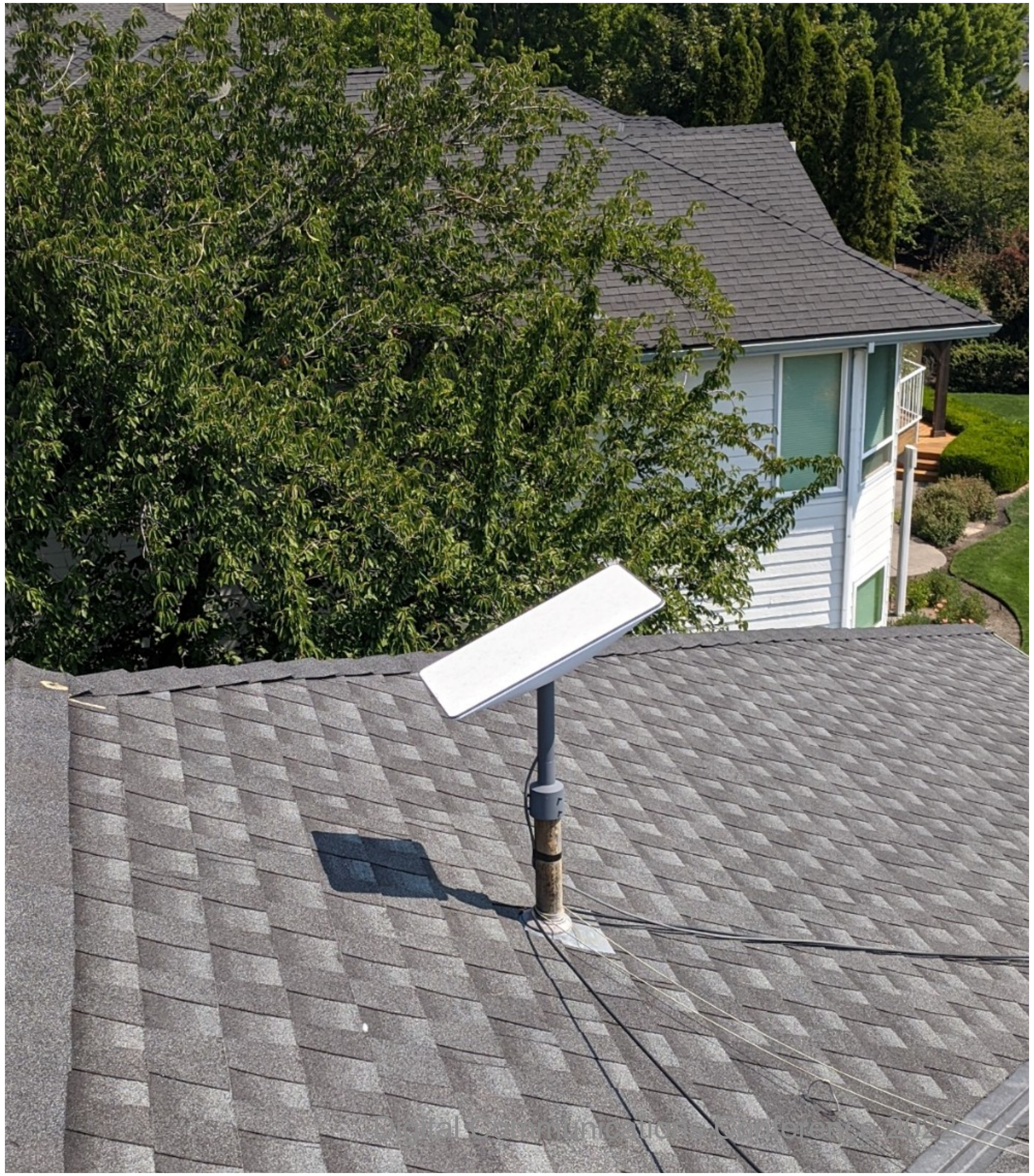
- Satellite Internet service offered by SpaceX (Elon Musk company).
- Provides fairly low-latency internet connectivity with a small portable flat phased-array dish.
    - In some places it’s the only reasonable Internet available.
- Uses a constellation of thousands of low-orbit satellites.
    - Satellite links you to a ground station.
    - A few Satellite-to-satellite laser links when ground station is not within range of the satellite.
- Phased-array electrical beam steering by the antenna to track rapidly-moving satellites.
- Capacity constraints occurring in busy areas (e.g. SF Bay Area).

Starlink Constellation – August 31, 2022



Starlink V2 ‘Dishy’: 12 inches x 20.25 inches.

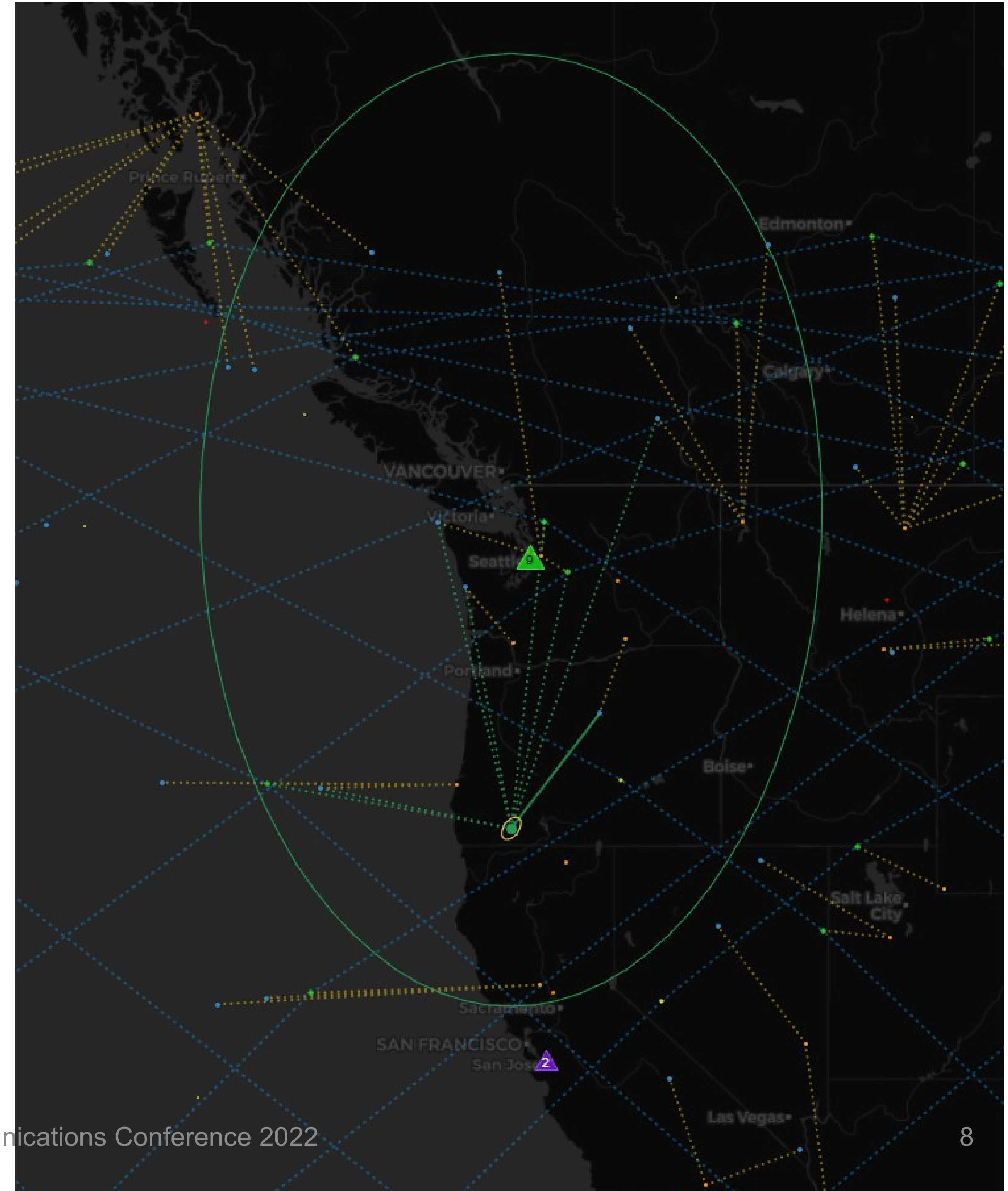
North ←



https://starlink.sx/

- Real-time visualization.

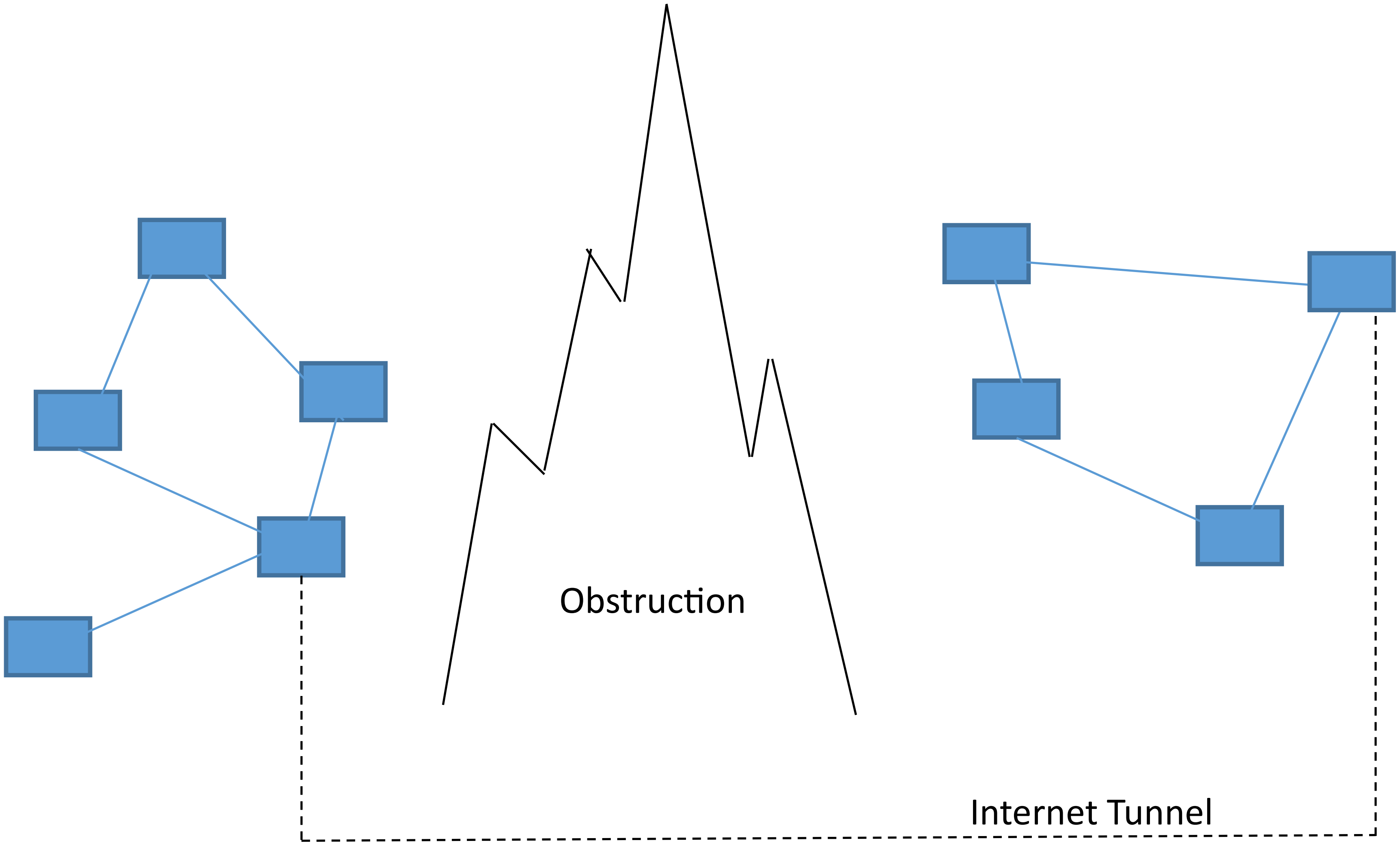
  https://starlink.sx/



Starlink to AREDN

- Starlink can be setup in many locations, providing high-speed Internet to mountain tops or other internet-less locations.
- It can provide a tunnel through the Internet from a remote AREDN node to your local node. AREDN uses TCP port 5525.
- It provides a way to temporarily establish AREDN connectivity while RF paths are being acquired, constructed, and put into service.
- AREDN-Starlink performance in the Rogue Valley network has been very good and pretty reliable.
- The AREDN node with Starlink service cannot easily be a tunnel server, it can easily be a tunnel client.

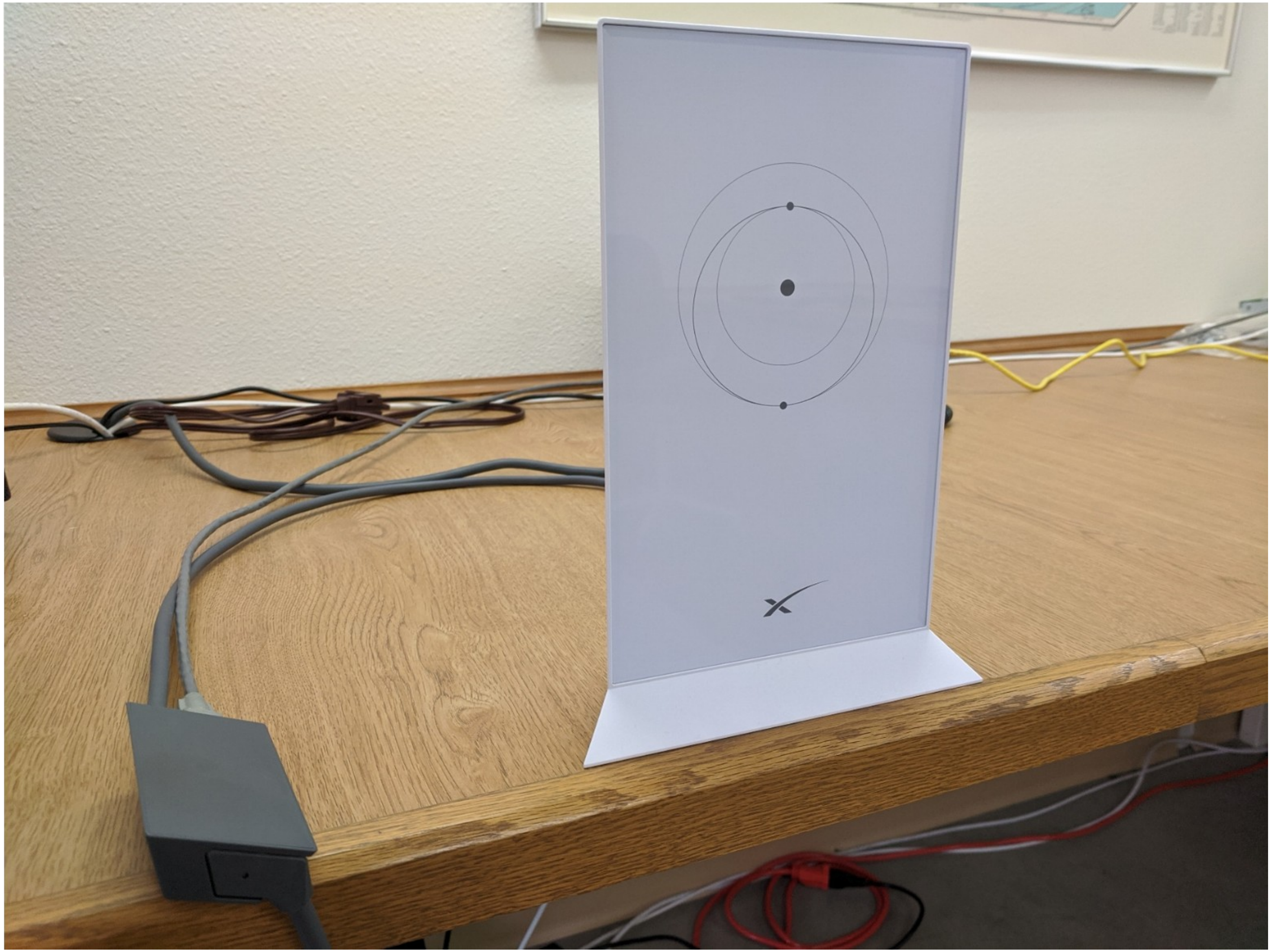
AREDN Tunnel Application



Starlink Issues

- Starlink has some major limitations.
- Standard Starlink does not provide a static or dynamic IPv4 address (the address your router is given is not routable).
  - It uses CG-NAT: Carrier Grade Network Address Translation, sometimes called NAT 444.
  - Allows one routable IPv4 address to be simultaneously shared by up to 128 different customers with each customer having many computers.
  - You have no control over IP address or port numbers, CGNAT entries time out.
  - Prevents running a service (e.g. cannot host a webpage, SSH, telnet, or AREDN tunnel server).
- Starlink is not currently supporting IPv6, but may in the future.

Starlink v2 Router plus Wired Ethernet Adaptor

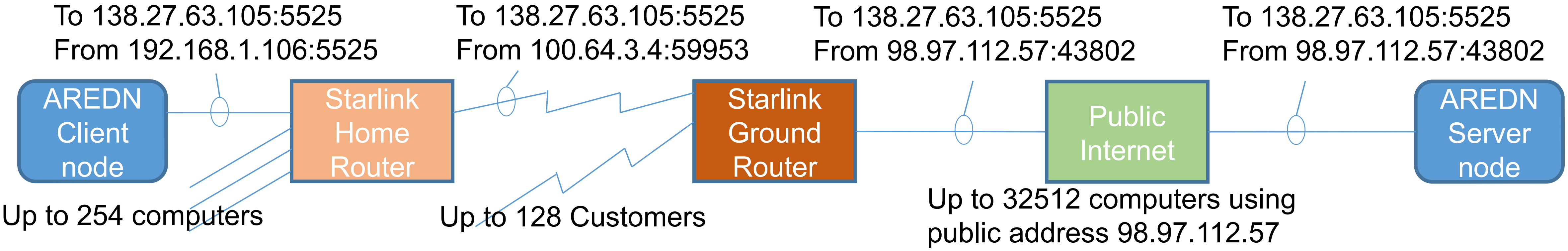


Starlink Issues - 2

- Starlink v2 Router – Provides Power-over-Cable to dishy and acts as router.
  - Default Configuration - Provides only WiFI.
  - Wired: Need to order separate Ethernet cable adapter ($20).
  - Issues DHCP dynamic addresses only in the 192.168.1.0/24 range.
  - Dish itself is at 192.168.100.1 (provides performance, statistics, obstructions, configuration).
- Can bypass Starlink home router with your own router.
  - You assume responsibility for DHCP or static IP addresses, NAT, routing, VLANs, Firewall, etc.
  - Must keep Starlink router connected to power the antenna, provide Ethernet connection.
  - Perhaps a delay getting the kind of router you want. Some IP routers back ordered > 1 year, no delivery date forecast.

A day in the life of a CG-NAT packet

100.64.0.0/10 is for CG-NAT: not publically routable.
5525 is the AREDN tunnel port number.



To 138.27.63.105:5525
From 192.168.1.106:5525

To 138.27.63.105:5525
From 100.64.3.4:59953

To 138.27.63.105:5525
From 98.97.112.57:43802

To 138.27.63.105:5525
From 98.97.112.57:43802

AREDN Client node

Starlink Home Router

Starlink Ground Router

Public Internet

AREDN Server node

Up to 254 computers

Up to 128 Customers

Up to 32512 computers using public address 98.97.112.57

The Client→Server works because the To: address and port number are unaltered from AREDN client towards the AREDN server.
The Internet knows how to route the packet to the AREDN server (To address).
The AREDN server replies back to the AREDN client by simply reversing the address:

To: 98.97.112.57::43802
From: 138.27.63.105:5525

The return path intervening nodes know how to unscramble the port number and resolve the original address. But CG-NAT table entries time out:

TCP typically 120 seconds for initial setup and 1800 seconds for inactivity.
UDP typically 30 seconds for initial setup and 120 seconds for inactivity.

Once timed-out, other computers and applications acquire those port numbers and the IP address. Now there’s no path back to the client from the server.

Starlink: AREDN Tunnel Server not reachable

- AREDN clients must know the IP address (or Domain name) of the AREDN server.
- Client contacts the server via known name and TCP port 5525.
- With Starlink providing Internet to the server:
  - Public Server name and port doesn't resolve to an end computer and port – no SRC-NAT table entries (128 different people resolve to one external IPv4 address).
  - Ports and IP are generated by Starlink, change periodically, are reclaimed and recycled based on idleness or other factors.
  - It's the same reason why you can't run a webserver using Starlink: no routable address + port number.
- Many wireless Internet providers also use CG-NAT.
  - They have the same issue.

Now What?

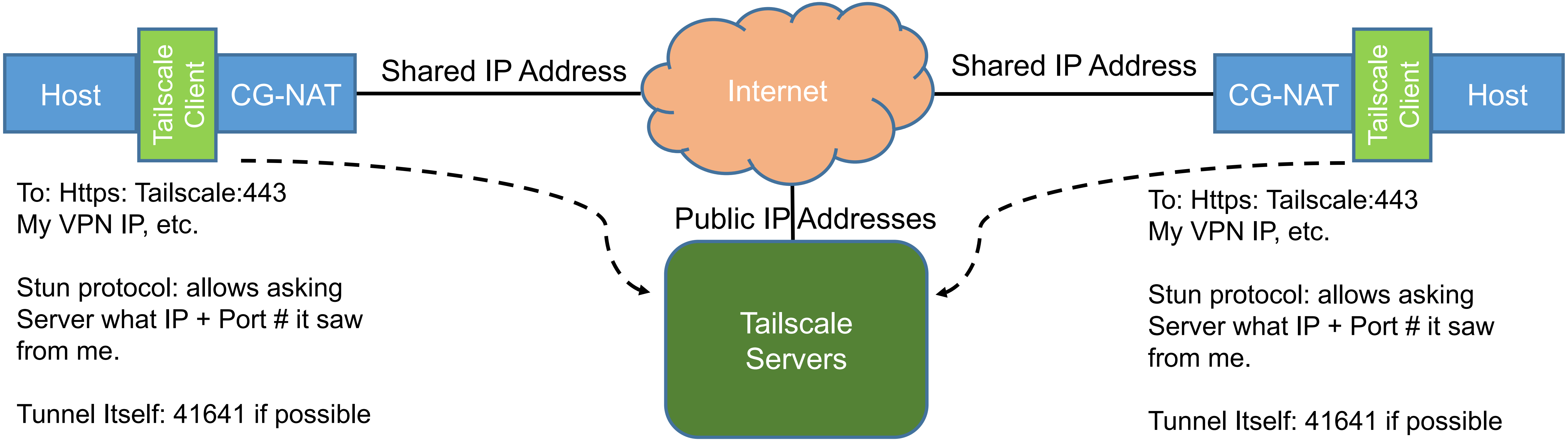
- Need a way to know the public IPv4 and port number of the server.
- Some Approaches:

1. Use a Virtual Private Network (VPN) to connect the client and server. VPN needs to externally resolve IPv4 and ports.
2. Use a cloud host to provide a public IPv4 and proxy the ports.

Tailscale VPN

- Tailscale is a VPN service. Free plan is good – up to 20 hosts, one subnet router, one management computer.
  - Very little configuration required – very easy to setup.
- Tailscale does not have knowledge of encryption or decryption keys. End devices responsible for holding their own keys, doing encryption, decryption (wireguard).
  - Install Tailscale software on hosts, authorize each via the management client.
  - Shows up as an additional Ethernet interface on the host.
- Tailscale handles dynamically finding and logging where each VPN device is in IPv4 space.
  - Dynamically leaks public addresses and ports from hosts to Tailscale's servers.
  - Keep alive: Periodically generates a tunnel packet to prevent CGNAT timeouts.
- Allows secure VPN access to home network via Starlink.
- Other VPN providers available (e.g. Cloudflare)

Tailscale



To: Https: Tailscale:443
My VPN IP, etc.

Stun protocol: allows asking Server what IP + Port # it saw from me.

Tunnel Itself: 41641 if possible

DERP: Digital End Relay Point for difficult CGNATs.

To: Https: Tailscale:443
My VPN IP, etc.

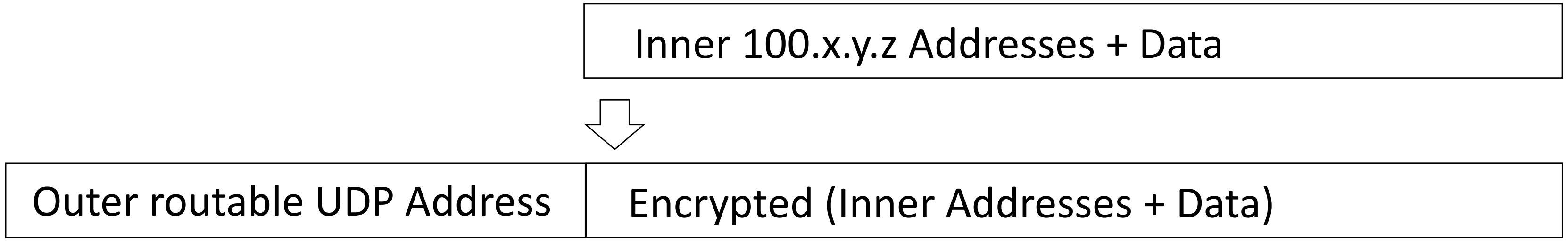
Stun protocol: allows asking Server what IP + Port # it saw from me.

Tunnel Itself: 41641 if possible

DERP: Digital End Relay Point for difficult CGNATs.

VPN Tunneling

- Tunneling encapsulates an entire IP packet including To / From address field with outer VPN UDP To / From address fields.
- The entire inner packet (100.64.0.0/10 unroutable address plus Data) is encrypted (wireguard)



Inner 100.x.y.z Addresses + Data

Outer routable UDP Address

Encrypted (Inner Addresses + Data)

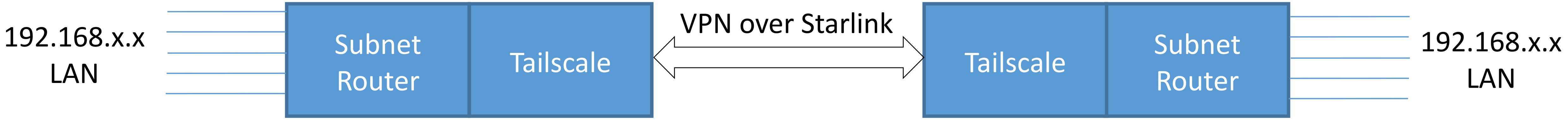
- The 100.64.0.0/10 address appears as an *additional* Ethernet interface on the host: tailscale0
- Tailscale figures out the routable address and port associated with each 100.x.y.z host address.
- VPN generates frequent keep-alive packets so that intermediate CG-NAT SRC-NAT VPN entries don’t time out.

VPN + Starlink

- When using Starlink-connected AREDN Server:
    - If AREDN client and server are on the same VPN they can connect.
- If Starlink-connected AREDN server is not on the same VPN as the client:
    - Then the client cannot reach the server.
- To make publically-available services when using Starlink we need a cloud host.
- Cloud host with:
    - Publically routable IPv4
    - And port forwarding with *static* SRC-NAT tables.
    - And joining the same VPN that the server is on.
- Once the general problem is solved then AREDN server works also.

Subnet Routers

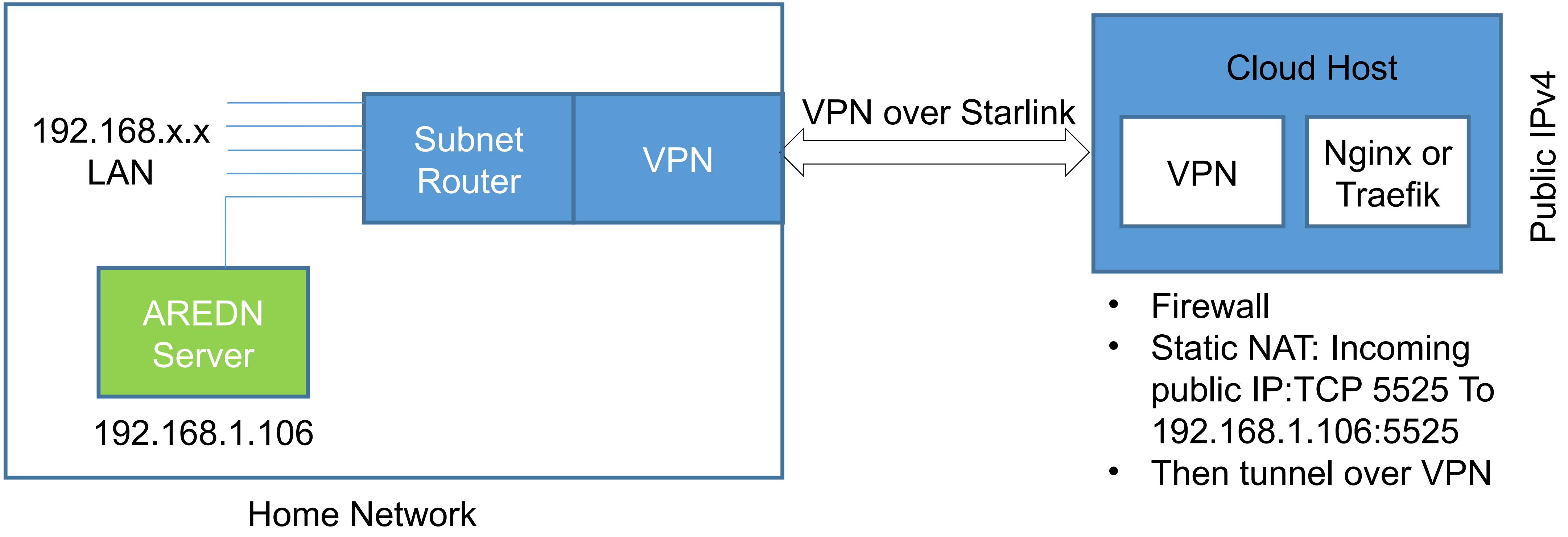
- Cannot install Tailscale VPN software on the AREDN node itself. Solution: use a subnet router to act on behalf of such devices on the LAN.
    - Subnet router advertises (multiple) address ranges
    - Connect devices such as printers, AREDN, etc. where Tailscale cannot be natively installed.
- Free (Personal) plan only includes one subnet router.
- Personal Pro allows 2 subnet routers. Cost: $48 / year



Cloud Host

- Numerous companies provide rent-a-host.
  - Linode, Vultr, Digital Ocean, etc.
  - Some in the $5 to $10 a month price range.
- The cloud host can get a static IPv4 address, it’s own ports.
  - Perhaps acquire a DNS name (about $10 / year) and register it in DNS.
- Install Tailscale VPN client on that host.
  - The cloud host has a Public IP address (DNS name), and
  - A private IP VPN address (that Tailscale knows about).
- Setup a reverse proxy on cloud host (Nginx or Traefik) to forward IP packets / port numbers through VPN tunnel to home network where they are run.
  - Reverse proxy holds NAT tables of port number / type to VPN network client IP and ports (e.g. port forwarding).
  - Allows you to provide local services (e.g. webpage) at known IP+port via cloud host.
  - Similarly setup AREDN tunnel port TCP 5525 to the AREDN server node.
- LocalXpose – service that provides hosted VPN + Reverse Proxy.
  - Free package very limited. $60/year plan is more useful.

Using a cloud host to establish public IP



- Firewall
- Static NAT: Incoming public IP:TCP 5525 To 192.168.1.106:5525
- Then tunnel over VPN

Conclusions

- Starlink provides a working AREDN client tunnel out-of-the-box.
  - No cloud host or VPN needed for client.
  - It has been working well for our network.
  - We’ve since overbuilt with 5 GHz mountain top links.
  - AREDN Tunnel is turned back on when radios or radio links fail.
  - Allows managing / reconfiguring / rebooting remote AREDN node.
- Try to have AREDN Server at a publically-reachable address.
  - Avoids VPN or Cloud Host requirement altogether.
- Providing an AREDN tunnel Server via Starlink requires both ends on the same VPN, or
- Requires a cloud host + reverse proxy if tunnel Server uses Starlink and Client is not on the same VPN as the server.