

Licensed to Experiment

Dan Norte WØBDP
Lucas Gahler NØOPS

Dan Norte | WØBDP



NetSPITM

- Principal Security Consultant
- 6 years occupational experience in Web Application, External Network, API, and Cloud penetration testing
- Licensed 9 years, now Amateur Extra
- Loves chasing DX and popping shells
- GLAARG, ARRL, Laurel Volunteer Examiner (VE)
- Drank the Yaesu kool-aid

Lucas Gahler | NØOPS

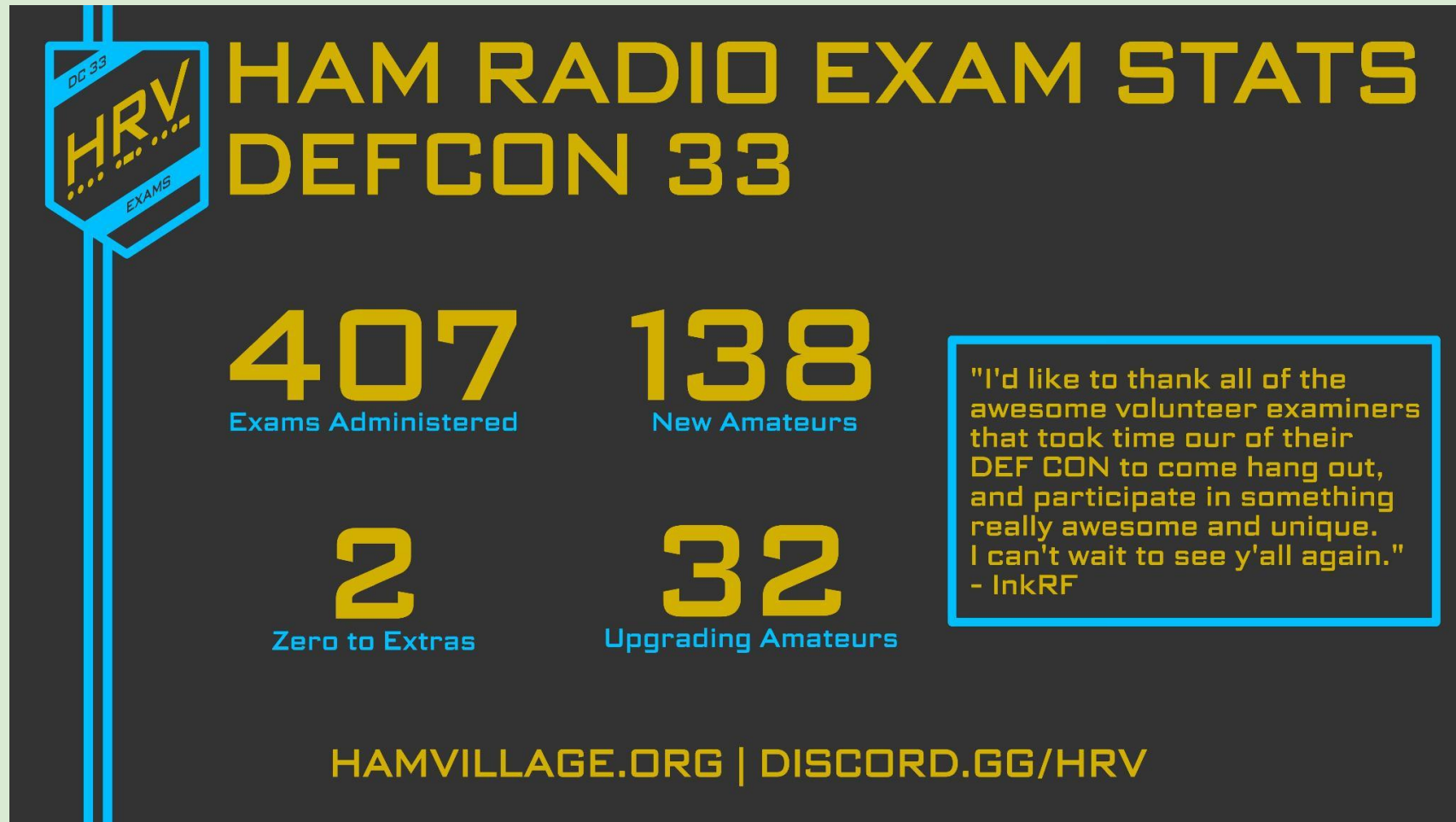


- 14 years in InfoSec
 - Security operations | vuln mgmt | DFIR | pentesting
- Licensed for 17 years, now Amateur Extra
- GLAARG and ARRL Volunteer Examiner (VE)
- Callsign is an accurate descriptor of my on-air operations
- Got Dan to drink the Yaesu kool-aid

Topics Covered

- How we ham radio
- The basic questions
- Broad discussion of aspects of the hobby
- Deep dive into some of our focus areas
- Example opportunities

Purpose of this talk



How we like to use our license



How we like to use our license



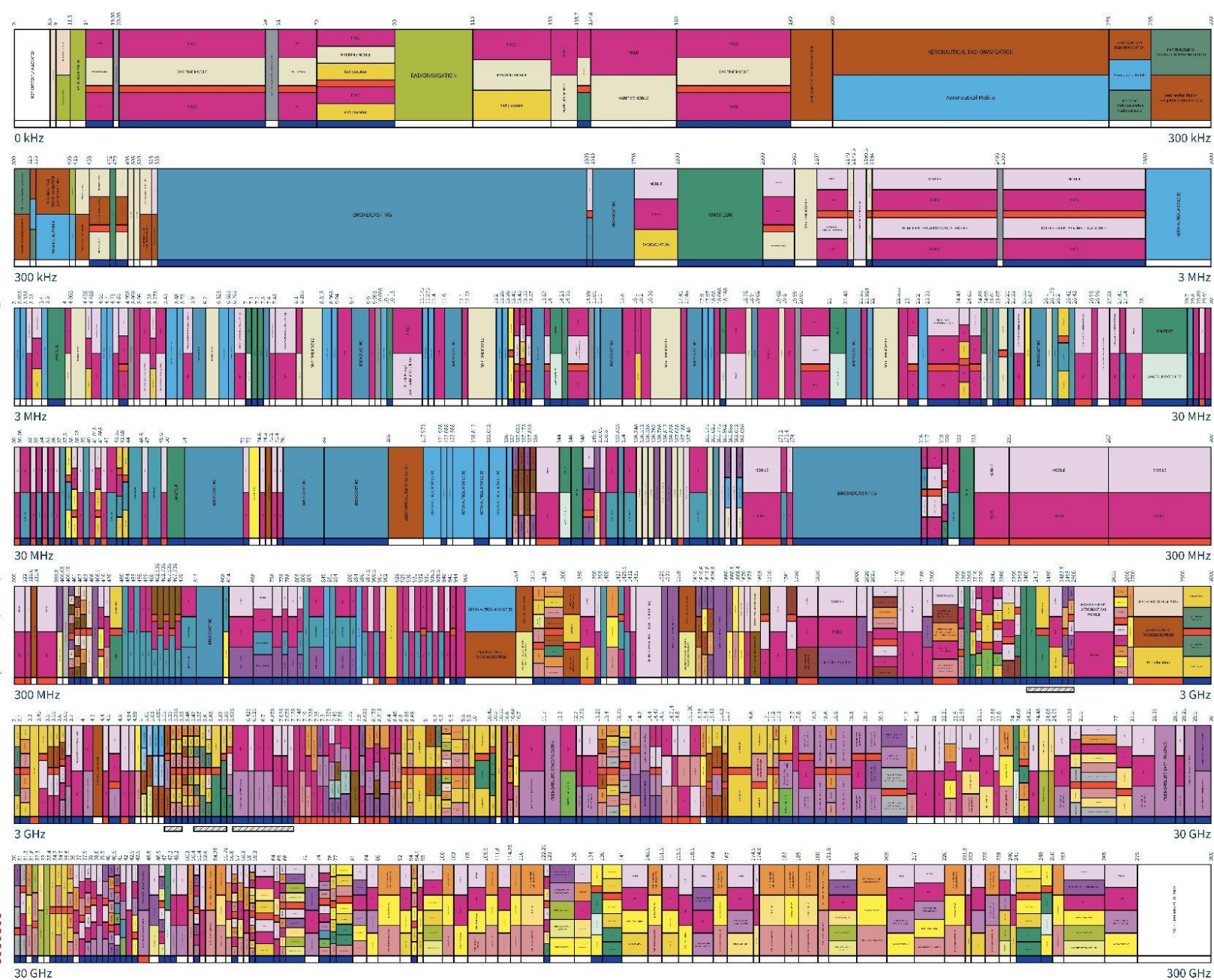


THE RADIO SPECTRUM

 Generalization Table In-situ Studies Self-assessment



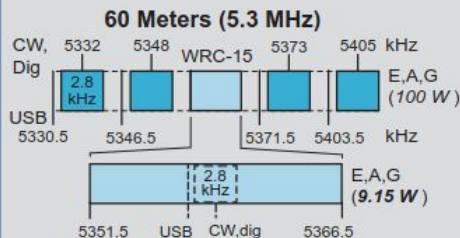
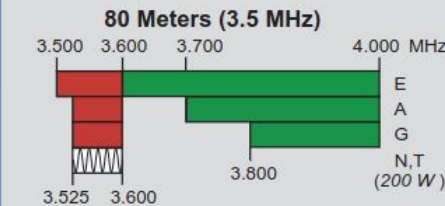
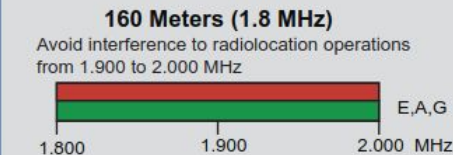
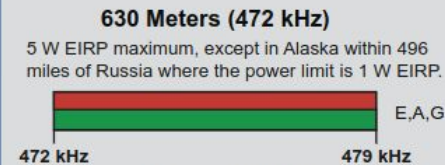
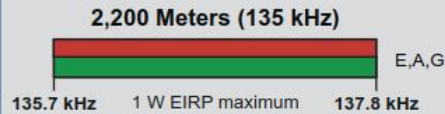
SERVICE	EXAMPLE	DESCRIPTION
Primary	100.1	Capitol, Interest
Secondary	Mobile	Initial capitol followed by decrease from 100



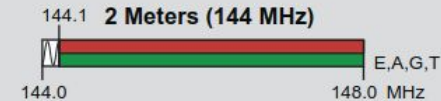
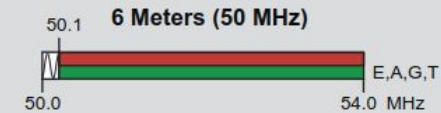
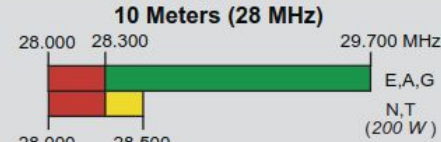
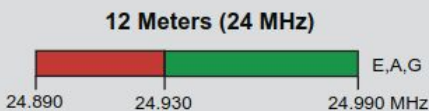
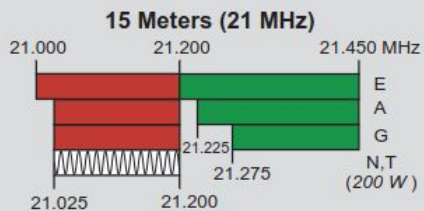
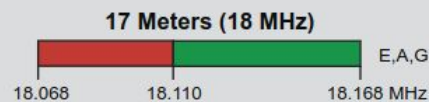
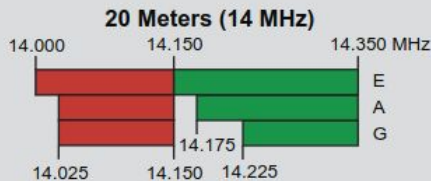
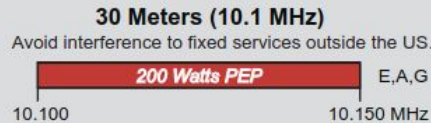
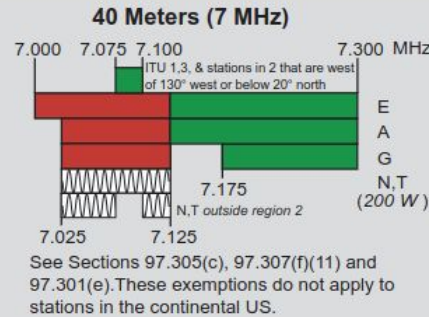
US Amateur Radio Bands

US AMATEUR POWER LIMITS — FCC 97.313 An amateur station must use the minimum transmitter power necessary to carry out the desired communications. (b) No station may transmit with a transmitter power exceeding 1.5 kW PEP.

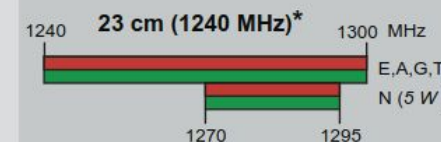
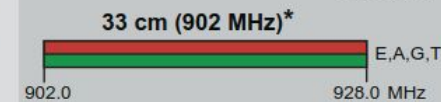
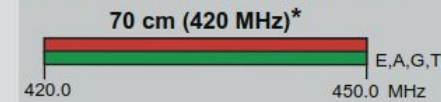
Amateurs wishing to operate on either 2,200 or 630 meters must first register with the Utilities Technology Council online at <https://utc.org/plc-database-amateur-notification-process/>. You need only register once for each band.



General, Advanced, and Extra licensees may operate on a secondary basis with an operating bandwidth of 2.8 kHz, maximum ERP of 100 W (relative to a half-wave dipole antenna) on individual channels. As February 13, 2026 the WRC-15 band 5351.5 to 5366.5 kHz is available with a max. ERP of **9.15 W**.



*Geographical and power restrictions may apply to all bands above 420 MHz. For information about your area, See FCC 97.303 Frequency sharing requirements.



All licensees except Novices are authorized all modes on the following frequencies:

2300-2310 MHz	10.0-10.5 GHz ‡	122.25-123.0 GHz
2390-2450 MHz	24.0-24.25 GHz	134-141 GHz
3300-3450 MHz	47.0-47.2 GHz	241-250 GHz
5650-5925 MHz	76.0-81.0 GHz	All above 275 GHz

‡ No pulse emissions



KEY

Note:

CW operation is permitted throughout all amateur bands.

MCW is authorized above 50.1 MHz, except for 144.0-144.1 and 219-220 MHz.

Test transmissions are authorized above 51 MHz, except for 219-220 MHz

- = RTTY and data
- = phone and image
- = CW only
- = SSB phone
- = USB phone, CW, RTTY, and data
- = Fixed digital message forwarding systems only

- E = Amateur Extra
- A = Advanced
- G = General
- T = Technician
- N = Novice

See www.arrl.org/band-plan for detailed band plans.

ARRL We're At Your Service

ARRL Headquarters:
860-594-0200 (Fax 860-594-0259)
email: hq@arrl.org

Publication Orders:
www.arrl.org/shop
Toll-Free 1-888-277-5289 (860-594-0355)
email: orders@arrl.org

Membership/Circulation Desk:
www.arrl.org/membership
Toll-Free 1-888-277-5289 (860-594-0338)
email: membership@arrl.org

Getting Started in Amateur Radio:
Toll-Free 1-800-326-3942 (860-594-0355)
email: newham@arrl.org

Exams: 860-594-0300 email: vec@arrl.org

Copyright © ARRL 2023 rev. 1/16/2026

The Opportunity

- It's the hobby of hobbies
- Virtually every aspect has opportunities for experimentation
- Hardware, protocols, OTA exchanges, etc



Two questions

- Who do you want to talk to?
 - The answer can be as abstract or profound as you want it to be
 - Anyone
 - “Nobody”
 - Subsets of people
- What is your goal?
 - Develop something novel/new
 - Personal skill building
 - Sample a little of everything vs specialize in one aspect

The Classics

- HF
- UHF/VHF
- Ragchewing
- Contests
- CW
- Fox hunting

n+OTA

- Summits on the Air (SOTA)
- Parks on the Air (POTA)
- Islands on the Air (IOTA)
- Get on the Air (GOTA)

Touch Grass

- World Wide Flora & Fauna (WWFF)
- Field Days
- ARES/RACES/Skywarn
- DX-peditions

Digital

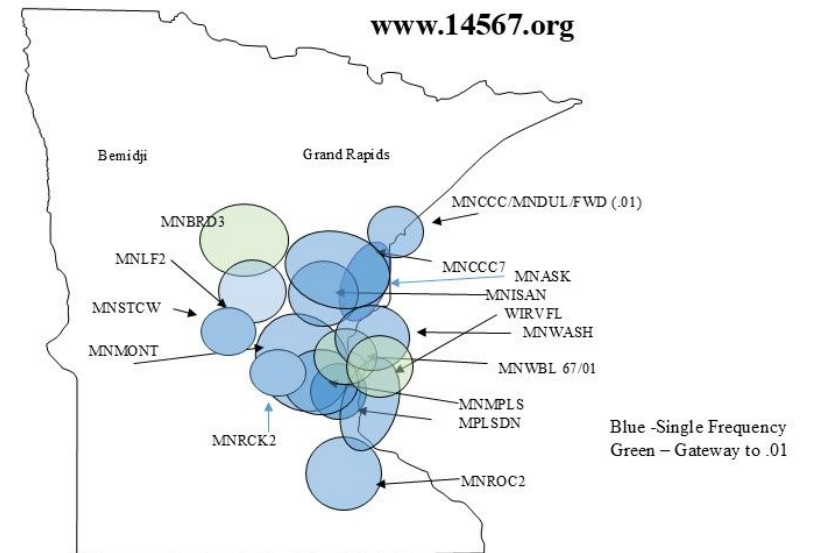
- FT8/FT4/FT2
- JS8Call
- No more 300 baud limit
 - Now 2.8 kHz bandwidth
- SSTV
- M17
- WSPR

Packet radio is still very much alive

- HF - check out Network 105 (14.105 LSB)
- Many areas have VHF packet networks
- Direwolf is on github
- Many radios come with built-in soundcards

7/25/25 MN 1200 bps Packet (145.67 MHz) Status

www.14567.org



The wide area stations are running unmodified Kantronics (KPC/3/4 and KAM/9612) TNCs with KA-Node®, open squelch, and watchdog timers at 1200 bps. We use Kantronics stock firmware. Emergency Operations Centers, ARES/Red Cross/Salvation Army emergency vans, etc. can run almost any TNC (Hardware or PC-soundcard) out of the box. There are no computers, TCP/IP or Internet links on the backbone nodes to reduce complexity/cost and rule out viruses/worms, unattended bulletin forwarding congestion and Internet distributed denial of service attacks. The primary traffic is keyboard-keyboard "instant" messaging, which requires less than 70 bits/second/user. These are mostly on commercial grade sites.

Source: hamtowertrailers.com

Aerospace

- ISS
- Satellites
 - (shout-out to SaveltForParts)
- EME moonbounce
 - Roundtrip path loss of 252dbi at 144mhz
- ADSB/ACARS/VDL/HFDL
 - airplanes.live
 - airframes.io
- Balloon tracking
 - sondehub.org
- Drones

Drones

- Video link requires license
- Likely factor in increasing license counts during last 7-8 years
- With new BVLOS (Beyond Visual Line of Sight) rules expected, legal opportunities for pushing higher ranges will become available

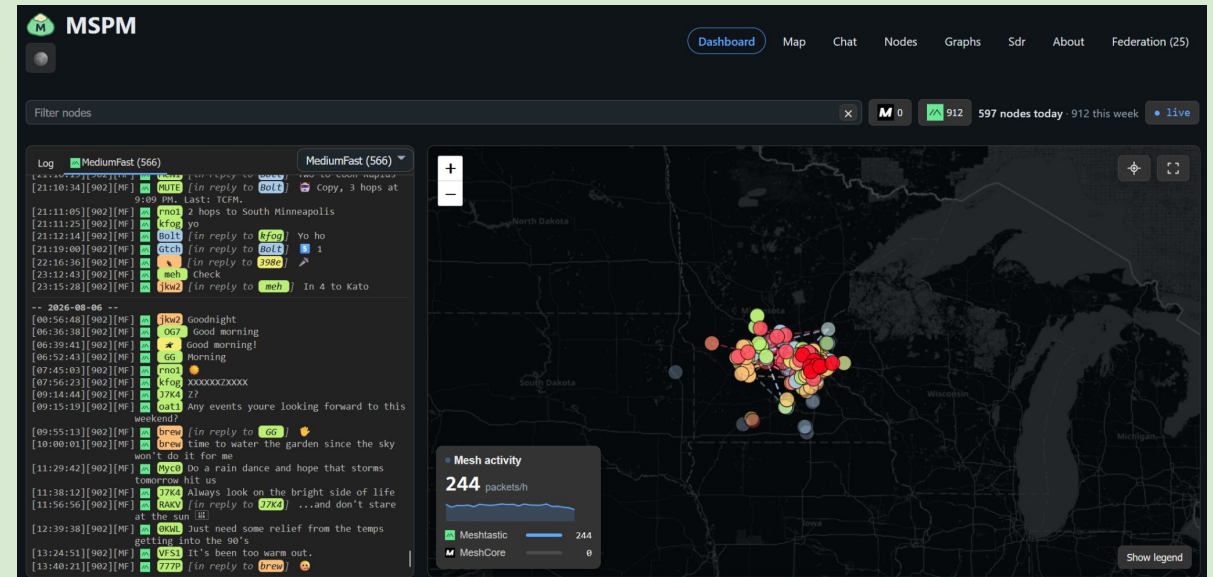
The Hobby Gateway Drug

- Soldering
- SDRs
- Antenna building
- Design/build your own radio
- Meshtastic/MeshCore



MSPMesh

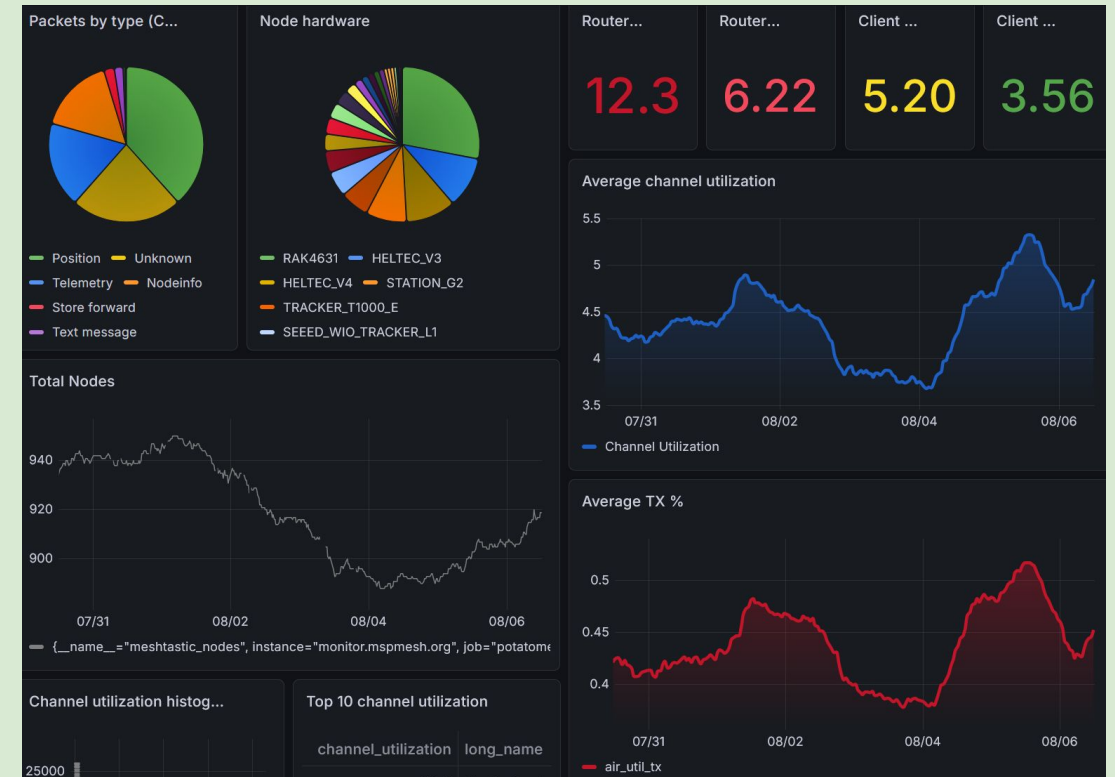
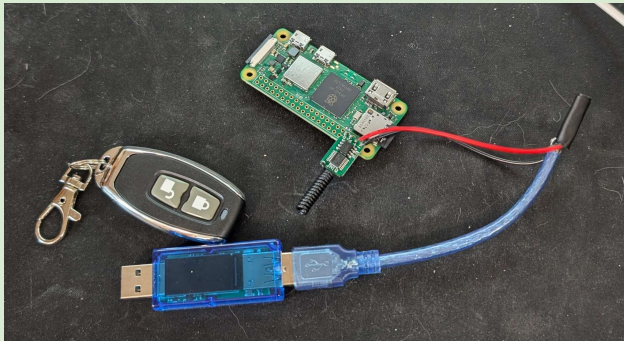
- June 2024 there were 8 of us
- Now ~900 daily active nodes
- 2000ish members in the Discord
- Approx 10% of members are licensed hamateurs
- No MQTT!



mspmesh.org

MSPMesh

- Potato-mesh
- Grafana dashboards
- Mesh-connected sticker printer
- Remote wifi updater



Antenna Building

- Everything can be an antenna
 - Can It Ham
 - Backyard gazebo
 - Ladders/fences
- $468 / f(\text{MHz}) = \text{Length}$
 - $468 / 7.15\text{MHz} = 65.45 \text{ ft}$ (half wave dipole)
 - $234 / 915\text{MHz} = 0.25 \text{ ft}$ (quarter wave whip)



>> | **Yagi** Change
High-gain directional beam with 2...

PARAMETERS

Design Frequency 12.800 MHz

Elements 6

Height 9.000 Unit: Meters (m) ▾

Element Diameter 7 mm

GROUND

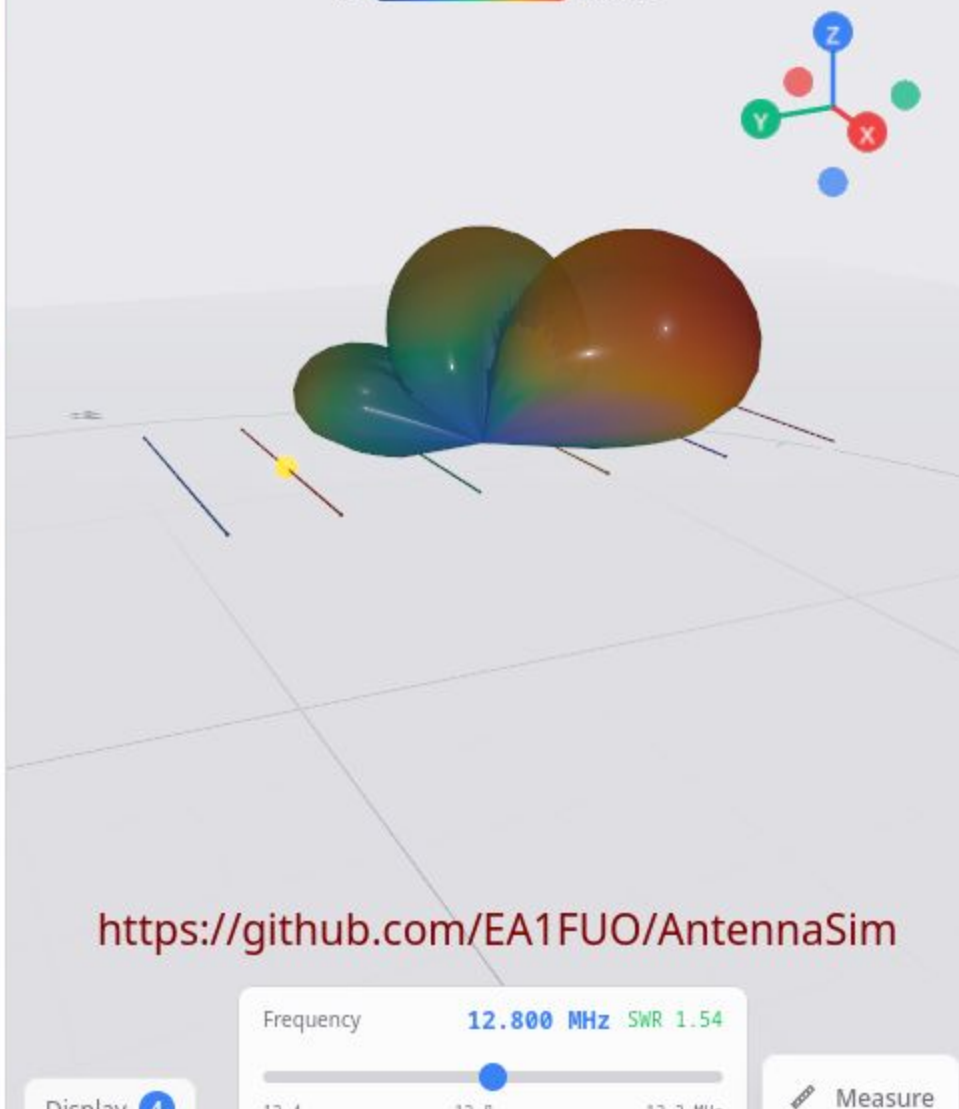
Average — $\epsilon_r=13$, $\sigma=0.005$ S/m

MATCHING

None (Direct 50 Ω)No matching, 50 Ω coax

BAND SWEEP PRESETS

?

Min  Max dBi<https://github.com/EA1FUO/AntennaSim>

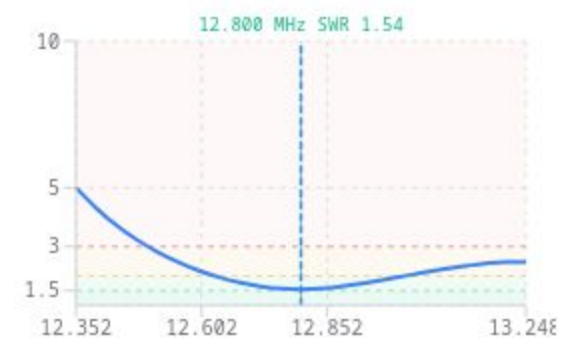
SWR Z Smith Pattern Gain Bands

SWR
1.54Gain
13.37 dBiImpedance
33.1 + j5.7 Ω

Export .s1p

SWR vs Frequency

.s1p



SWR (simulated)

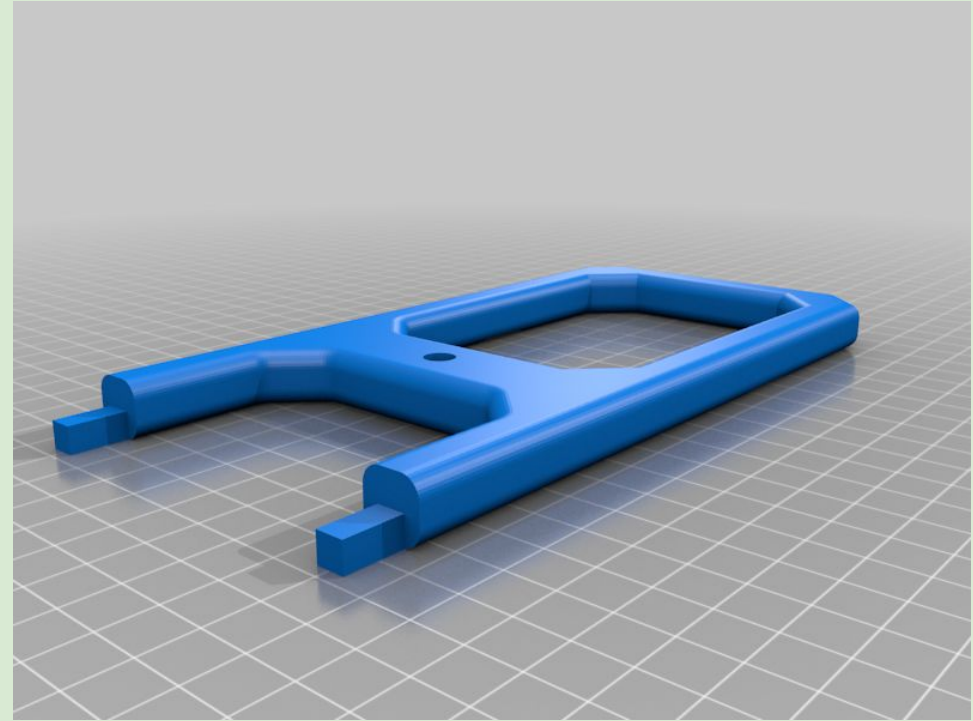
● <1.5 Good ● 1.5-3 OK ● >3 Poor ... Resonance

Frequency 12.800 MHz SWR 1.54

Display 4

Measure

3D Printing



<https://www.thingiverse.com/thing:5521016>

Development

- Resume builder - open source projects
- Make \$\$\$

Development - Open Source

- <https://github.com/iaru-r1/opensource-projects>
 - Firmware
 - Logging
 - Modes
 - Remote Control
 - Software Defined Radio
 - Morse Code
 - Standards
 - Education

Let's Talk Money



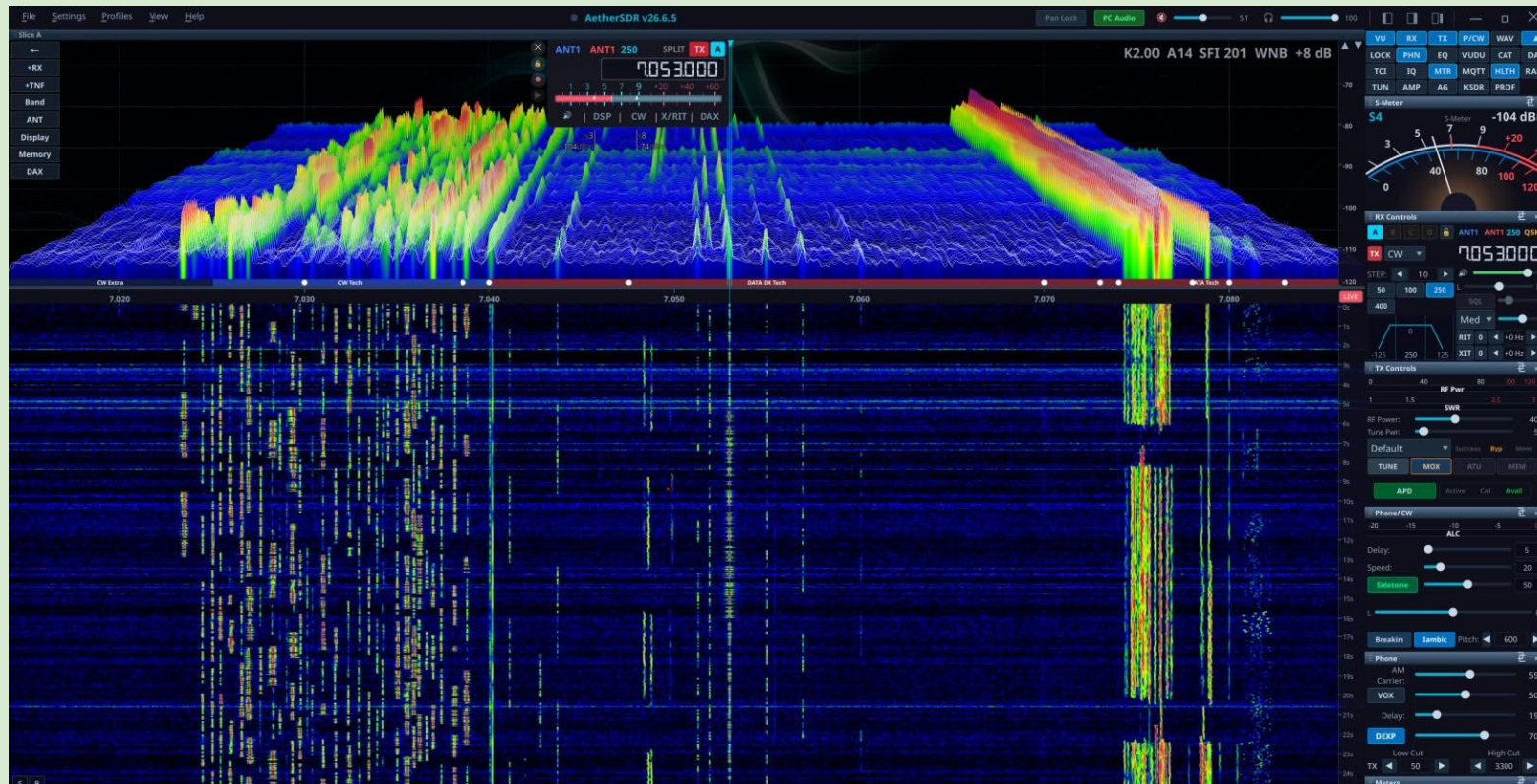
The Flex

- Software Defined Radio using SmartSDR
- Samples 30 kHz to 54 MHz
- Allows monitoring of up to 8 frequencies at once
- MSRP \$9,599
- iOS app \$79.99



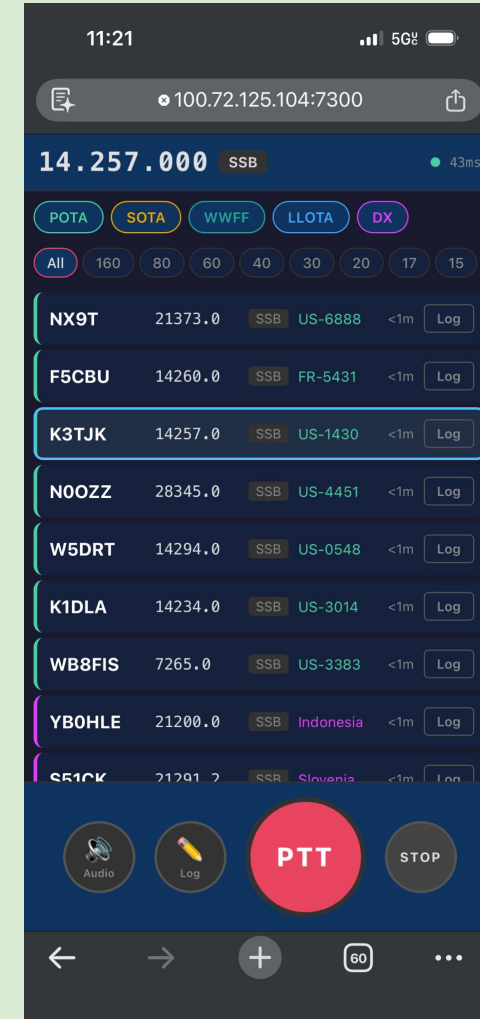
You're Too Late For \$\$\$

- <https://github.com/aethersdr/AetherSDR>



POTACat - Remote Control

- <https://potacat.com/>
- Unified spotting to help complete POTA/SOTA/DX
- Aims to remote control all the radios
- Tailscale + ECHOCAT for mobile



You're Too Late For \$\$\$, Almost

lose my
money!



Where's my android
app!?

Content Creation

- Small, but captive audience
- <https://www.youtube.com/@HamRadioK8FAE>
- <https://www.youtube.com/@shesonfrequency>

My Callsign is My Passport

- Our Defcon 31 talk (@HamRadioVillage):
<https://www.youtube.com/watch?v=1FKAdsJGAbs>
- Slide deck:
<https://github.com/mycallsignismypassport/DC31-HRV>

What We Found

Summary of Findings:

- 6 HIGH Vulnerabilities
- 3 MEDIUM Vulnerabilities
- 3 LOW Vulnerabilities
- 1 Informational Vulnerability



Estimated Effort: 12.5 hours!

Any Questions?