

A Hacker's Journey in Ham Radio

DC402 – December

zonksec – tyler rosonke

ham radio == amateur radio?

- The term "ham" was first a pejorative term used in professional wired telegraphy during the 19th century, to mock operators with poor Morse code-sending skills ("ham-fisted")
- This term continued to be used after the invention of radio and the proliferation of amateur experimentation with wireless telegraphy; among land- and sea-based professional radio operators, "ham" amateurs were considered a nuisance.
- The use of "ham" meaning "amateurish or unskilled" survives today sparsely in other disciplines (e.g. "ham actor").

why interested in ham radio at all?

- movies / pop culture
- always curious about it
- never knew what it “really” was



why interested in ham radio at all?

- Kinda similar to hacking
 - curious people
 - tinkerers
 - can be technical
 - DIY / hands-on



So where to start?

- Lots going in the hobby and thus generic googling is confusing
- One thing was for certain, an FCC license is needed to legally transmit.
- So that's where I started!
 - Got my technical license in 2017 (proctored local exam)
 - Studied for about a week or two with hamstudy.org (423 Qs in pool, 35 on exam)
- Now what?

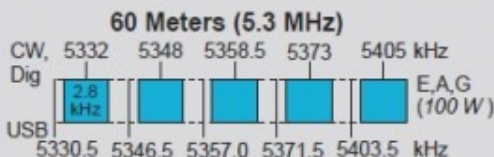
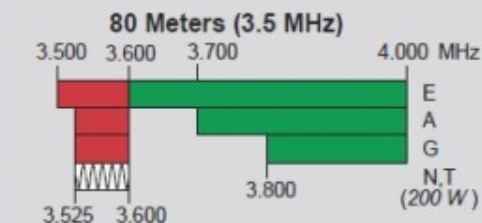
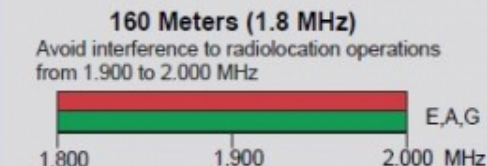
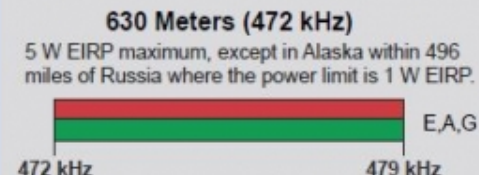
US Amateur Radio Bands

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.

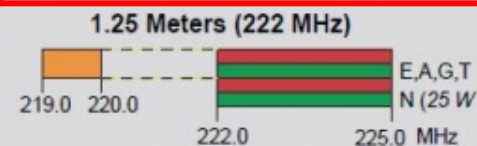
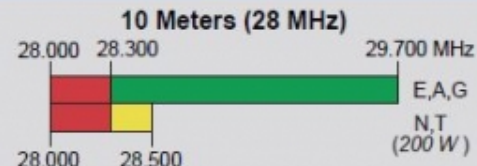
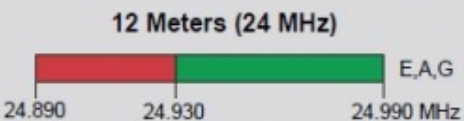
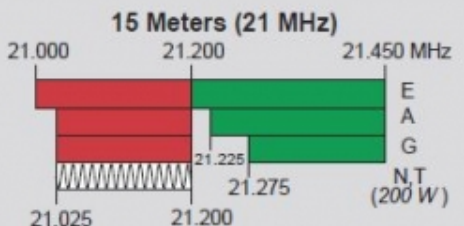
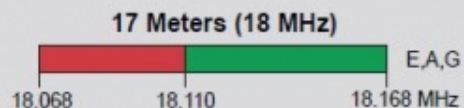
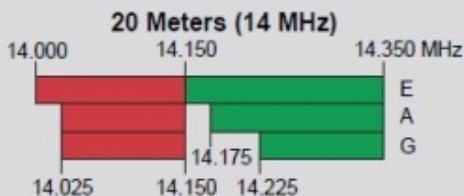
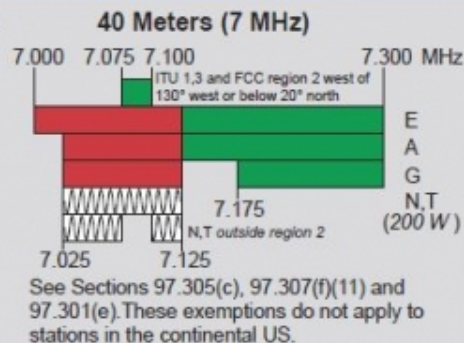


ARRL The national association for AMATEUR RADIO®

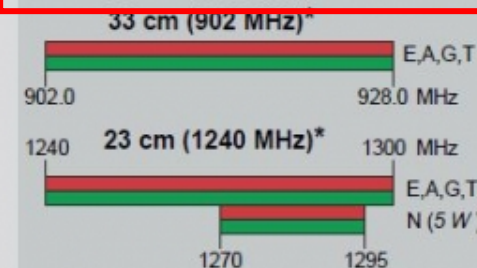
Amateurs wishing to operate on either 2,200 or 630 meters must first register with the Utilities Technology Council online at <https://utc.org/plc-database-amateur-notification-process/>. You need only register once for each band.



General, Advanced, and Amateur Extra licensees may operate on these five channels on a secondary basis with a maximum effective radiated power (ERP) of 100 W PEP relative to a half-wave dipole. Permitted operating modes include upper sideband voice (USB), CW, RTTY, PSK31 and other digital modes such as PACTOR III. Only one signal at a time is permitted on any channel.



*Geographical and power restrictions may apply to all bands above 420 MHz. See The ARRL Operating Manual for information about your area.



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
3300-3500 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 **ARRLWeb** at www.arrl.org 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

VHF/UHF radio

- The famous/infamous Baofeng UV-5R
 - \$25
 - Perfect for if you are not sure if the hobby is for you!

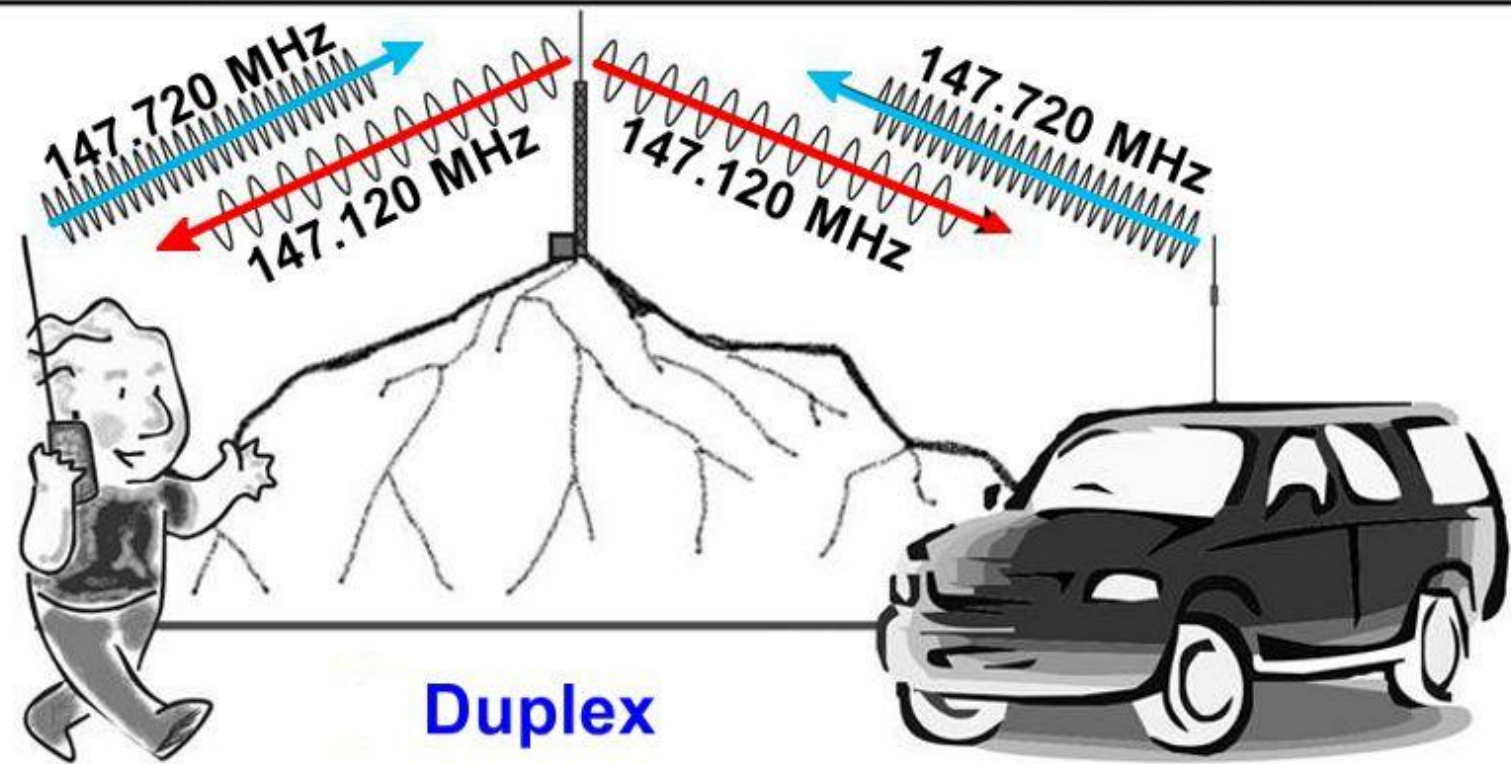
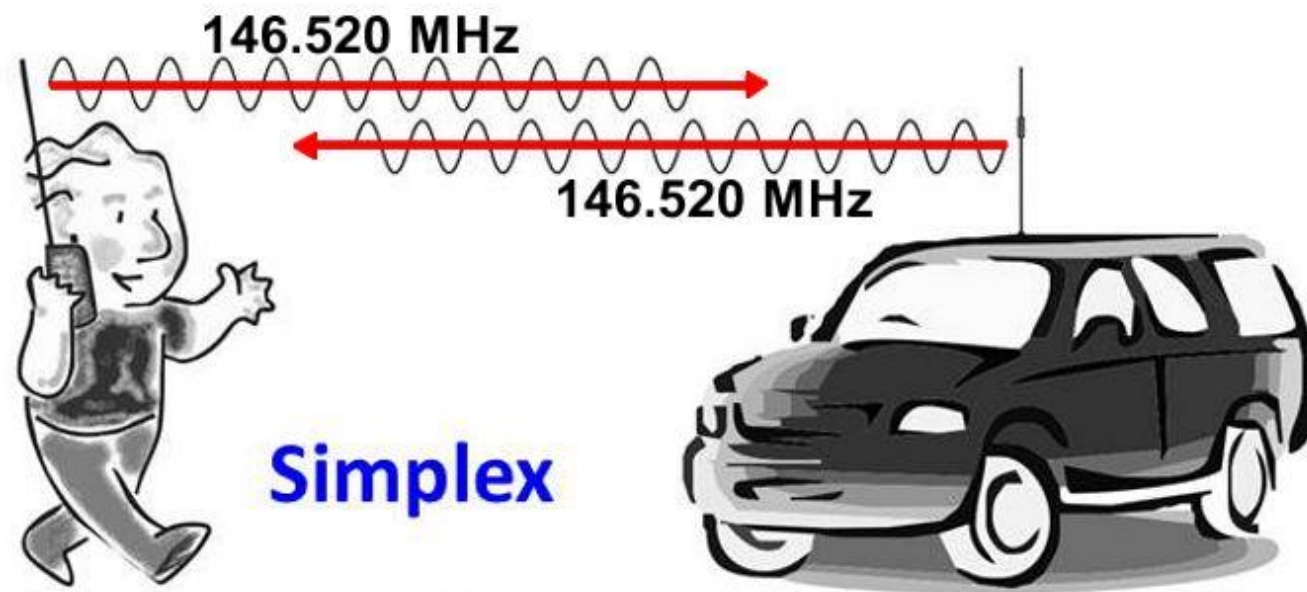


Range

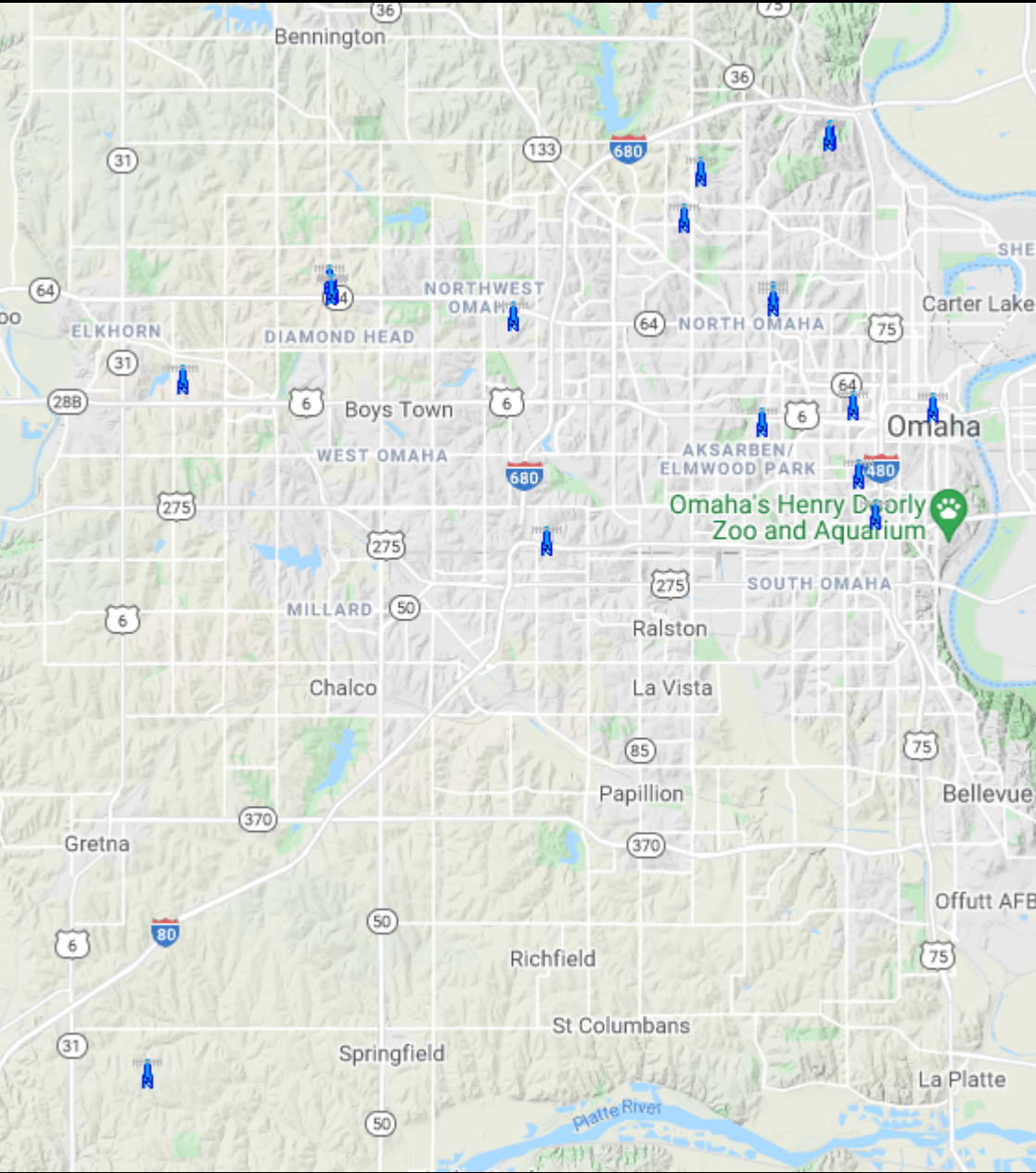
- Can I talk
- ☹ not r
- VHF/UHF
 - At ~5



3miles



Frequency	Offset	Tone In / Out	Location	County	Call	Use	Modes
145.1750	-0.6 MHz		Omaha	Douglas	KD0CGR	OPEN	DSTAR
145.3700	-0.6 MHz		Omaha, CHI Immanuel Hospital	Douglas	N0YMJ	OPEN	FM
145.4500	-0.6 MHz	131.8	Omaha	Douglas	K0BOY	OPEN	FM
146.9400	-0.6 MHz		Omaha, KETV Tower (Crown Point)	Douglas	K0USA	OPEN	FM
147.0000	-0.6 MHz		Omaha	Douglas	WB0CMC	OPEN	FM
147.0000	+0.6 MHz		Omaha	Douglas	WB0CMC	OPEN	FM
147.3000	+0.6 MHz	CSQ / CSQ	Omaha	Douglas	WA0WTL	CLOSED	FM
147.3600	+0.6 MHz		Omaha, Douglas County Communications Center	Douglas	K0BOY	OPEN	FM
223.5800	0 MHz	100.0 / 100.0	Omaha, Mormon Bridge	Douglas	K0OQL	OPEN	FM IRLP
224.7600	-1.6 MHz	146.2	Omaha	Douglas	WB0YLA	OPEN	FM
421.2500	+12.75 MHz	ATV	Omaha, Benson High School	Douglas	WB0CMC	OPEN	ATV
442.1250	+5 MHz		Omaha	Douglas	KD0CGR	OPEN	DSTAR
442.2250	+5 MHz	136.5 / 136.5	Omaha, WOWT TV Tower 36 + Farnam	Douglas	K0SWI	OPEN	FM Fusion
442.3250	+5 MHz	100.0 / 100.0	Omaha, Hefflinger Park	Douglas	KW1RKY	OPEN	FM EchoLink
442.4750	+5 MHz	100.0 / 100.0	Omaha	Douglas	KA0IJY	OPEN	FM
442.6500	+5 MHz	CC1	Omaha	Douglas	K0BOY	OPEN	DMR
442.8250	+5 MHz	CC1	Omaha, Douglas County Communications Center	Douglas	WB0QQK	OPEN	DMR
442.9500	+5 MHz	146.2 / 146.2	Omaha	Douglas	KC0YUR	OPEN	FM
443.4500	+5 MHz	100.0 / 100.0	Omaha	Douglas	KB0SMX	OPEN	FM
443.7250	+5 MHz	100.0	Omaha	Douglas	KF6SWL	OPEN	FM
443.7750	+5 MHz		Omaha, KPTM/KXVO TV Tower	Douglas	W0EQU	OPEN	FM
443.9250	+5 MHz	103.5 / 103.5	Omaha	Douglas	KG0S	OPEN	FM AllStar



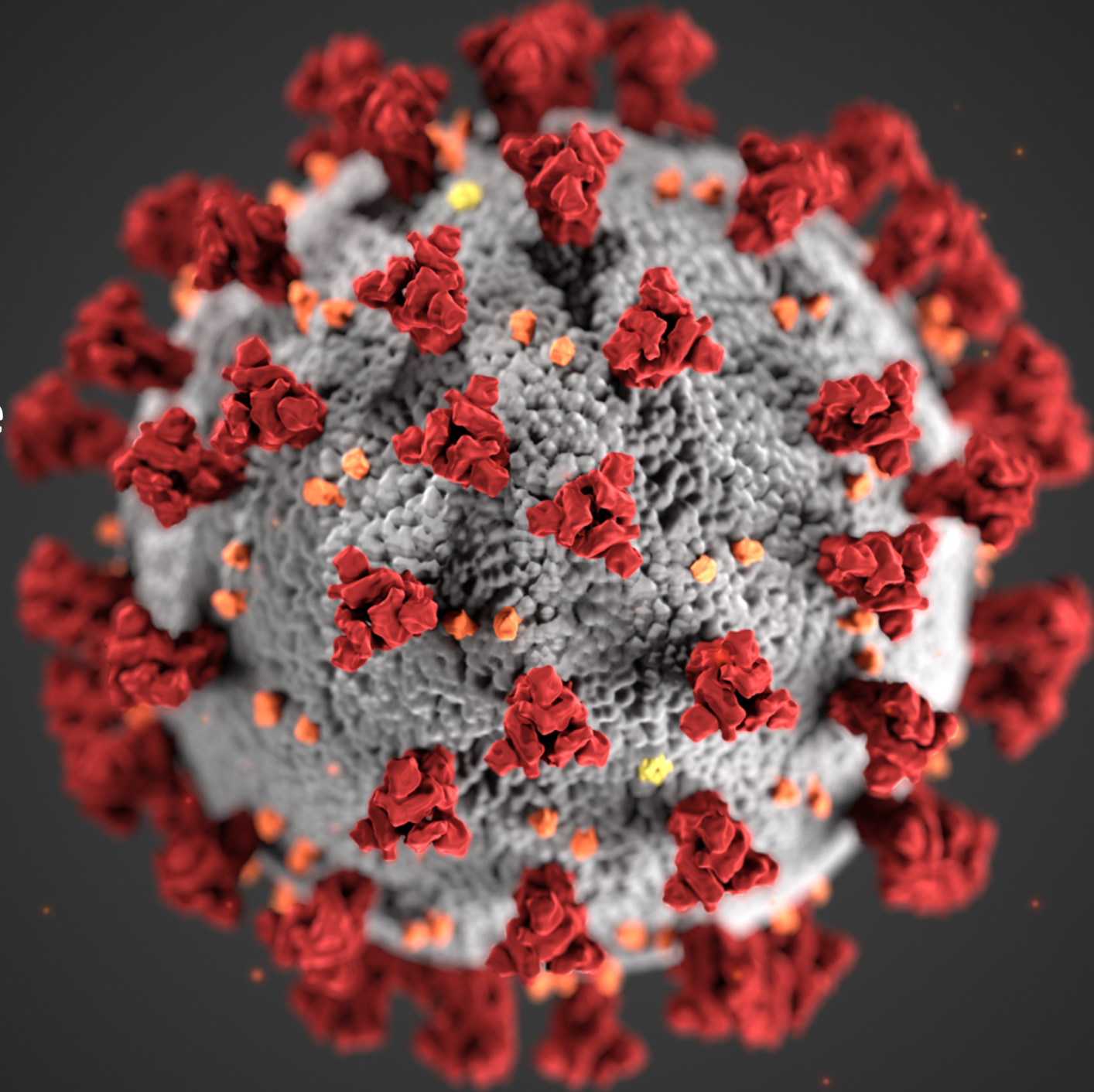
interest fades

- It was fun configuring my radio and had fun learning all the new things so far...

BUT

- My current license doesn't let me do the things movies showed me
- Those things are new and confusing
- And to do those things, I need more expensive equipment.
- Couldn't find my personnel "point". Now what?

2020 =
the perfect time
to dive in
further!



So where to start?

- Another round of ham study and got my general license
- (did it via webcam in my bathroom)

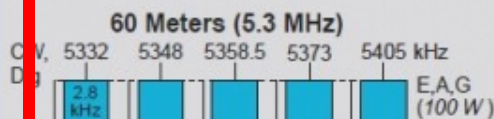
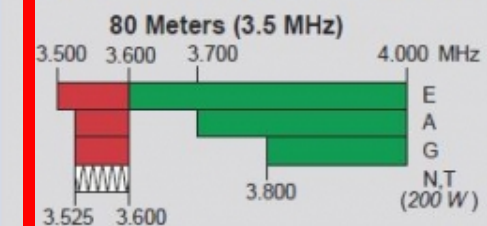
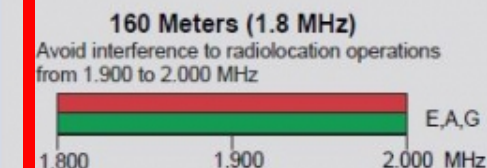
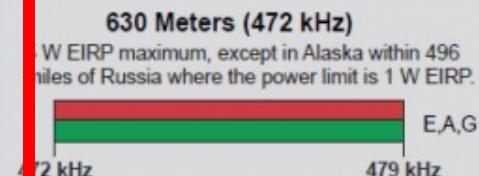
US Amateur Radio Bands

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.

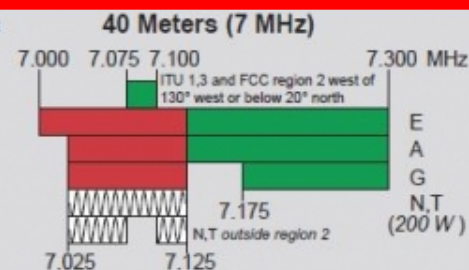


ARRL The national association for AMATEUR RADIO®

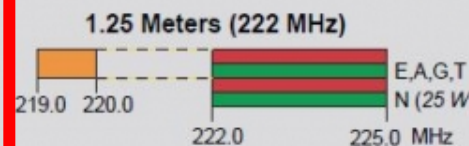
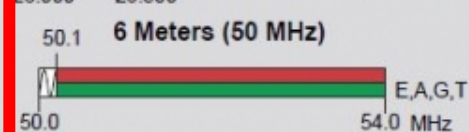
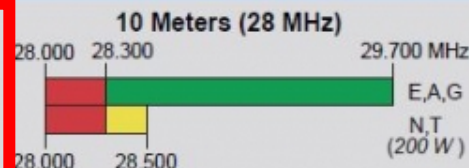
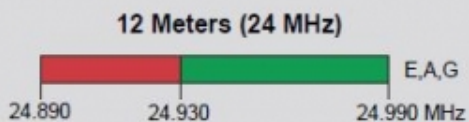
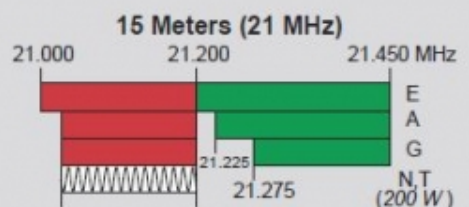
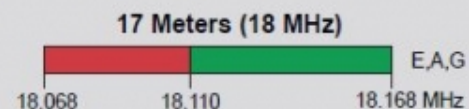
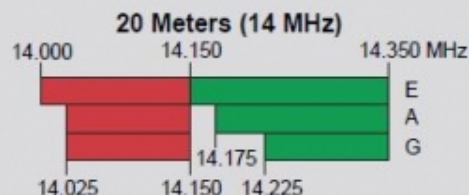
Amateurs wishing to operate on either 2,200 or 630 meters must first register with the Utilities Technology Council online at <https://utc.org/plc-database-amateur-notification-process/>. You need only register once for each band.



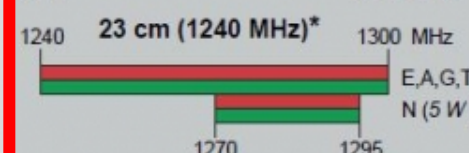
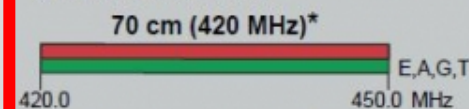
General, Advanced, and Amateur Extra licensees may operate on any channel on a secondary basis with a maximum effective radiated power (ERP) of 100 W PEP relative to a half-wave dipole. Permitted operating modes include upper sideband voice (USB), CW, RTTY, PSK31 and other digital modes such as PACTOR III. Only one signal at a time is permitted on any channel.



See Sections 97.305(c), 97.307(f)(11) and 97.301(e). These exemptions do not apply to stations in the continental US.



*Geographical and power restrictions may apply to all bands above 420 MHz. See The ARRL Operating Manual for information about your area.



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
3300-3500 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 **ARRLWeb** at www.arrl.org for detailed band plans.

ARRL We're At Your Service

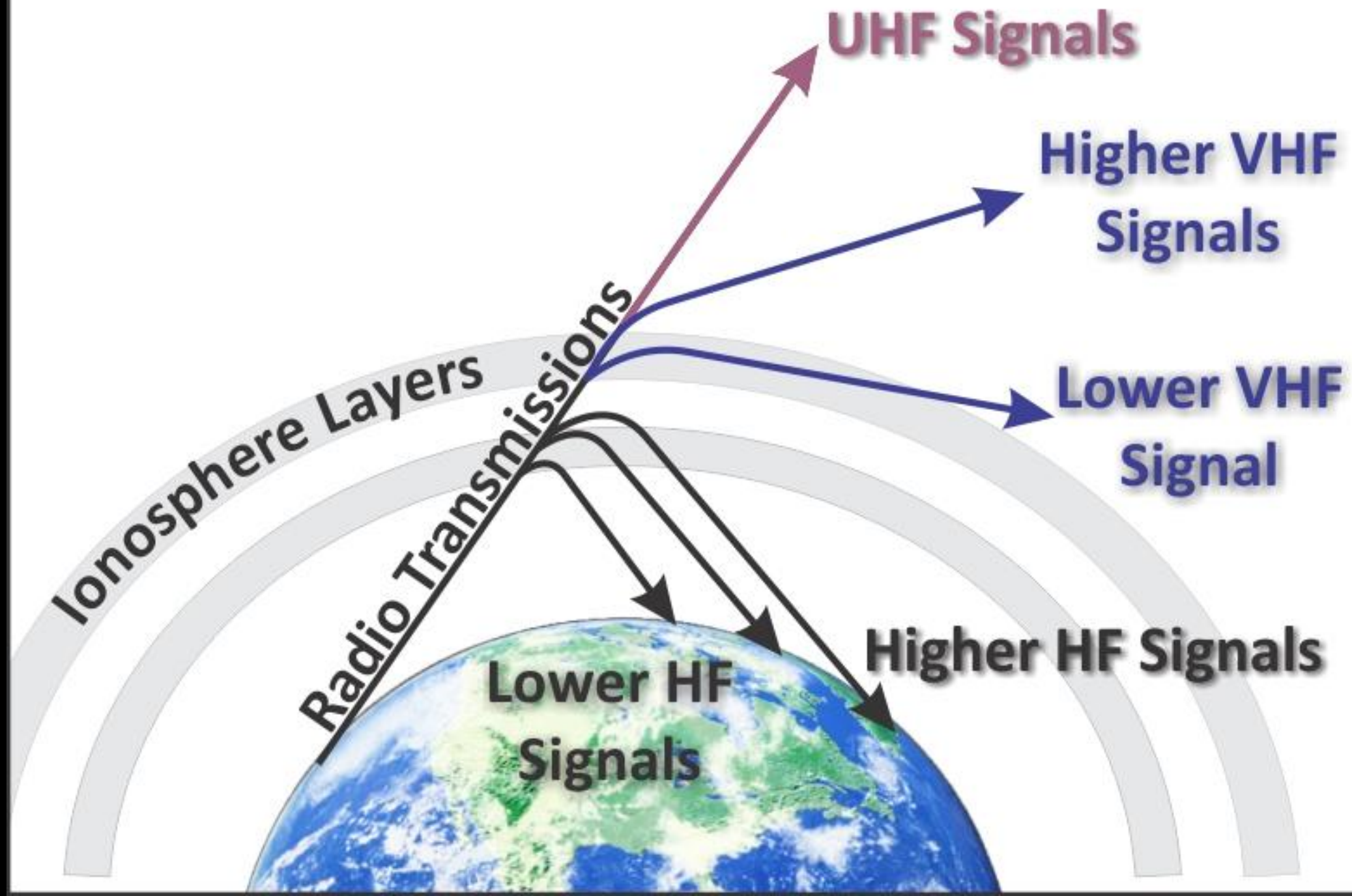
ARRL Headquarters:
860-594-0200 (Fax 860-594-0259)
email: hq@arrl.org

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

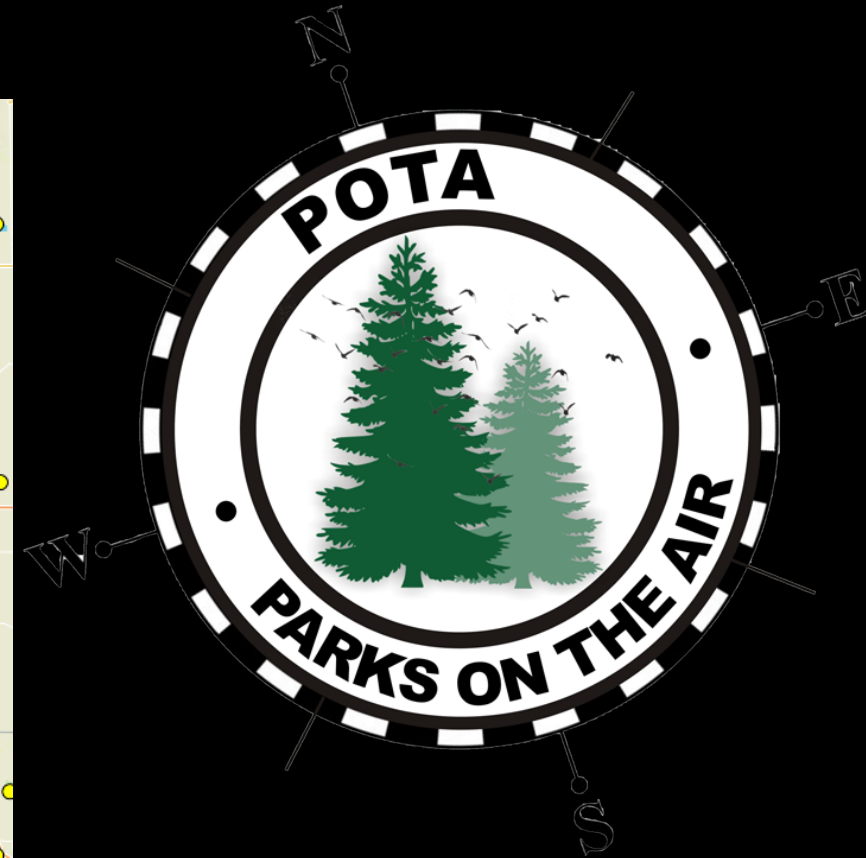
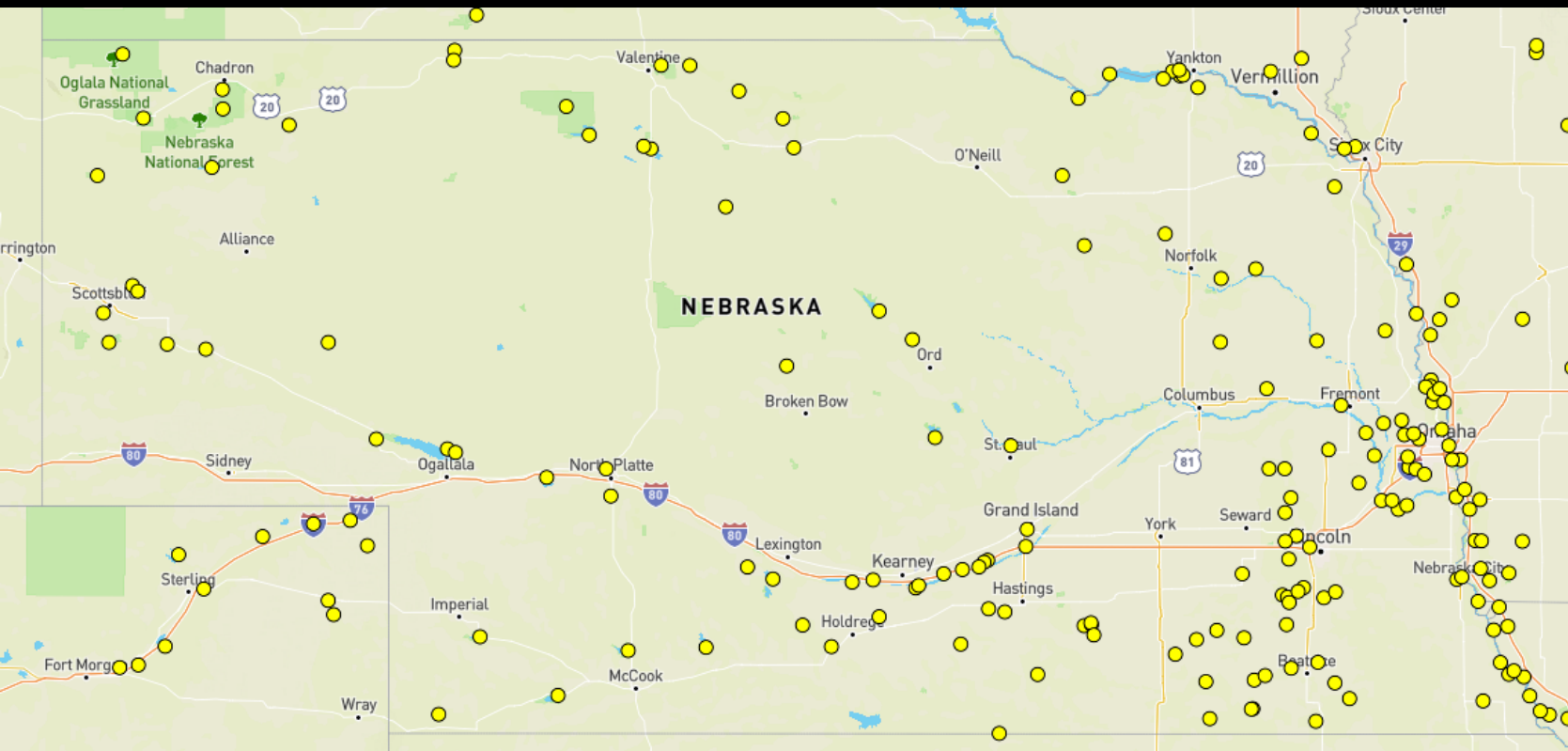


But what about the “now what” problem?

- wont I have the same problem? Just talking with people further away? what's the point?
- while poking around during exam study, I came across something that became the X factor for my experience with ham radio...

Parks on the Air (POTA)

- Activate Parks
 - Go to designated parks (county, SRAs, national), setup up station, make contacts. (10 = activated)
- Hunt Parks
 - Stay home, try to talk to people out in parks.



Bought HF Radio Gear

- XIEGU G90
 - ~\$440
 - Not the cheapest way to get on HF. But it fit the bill for POTA.
 - Portable – very small and light
 - Great builtin ATU – no addon gear needed
 - SDR – very configurable
 - Can be powered by RC lipos



Parks on the Air (POTA)

- Gamification!
- Emphasis on contacts / technical outcomes, not “rag chew”
- Logistics is fun
 - How far can you go? How quickly can you process the pile up? How will you setup portal station? What route is most efficient? Where in the park is easy to access? 2fers?



 main ▾ 1 branch 0 tags

Go to file

Add file ▾

Code ▾



ZonkSec Update README.md

70d6232 9 days ago  8 commits

README.md

Update README.md

9 days ago



callsign2usstate.py

init commit

25 days ago



parksTODOgps.py

init commit

25 days ago



potalog2adif.py

Create potalog2adif.py

9 days ago



usstateCompleteCheck.py

init commit

25 days ago



README.md



POTA-ham-scripts

these are some ham radio scripts i wrote for POTA purposes. converting logs, checking for various things, etc

they are quick and dirty, room for improvements everywhere, but they help me see if ive reached my goals!

callsign2usstate.py

this script takes a file path to an ADIF file and then converts all QSO callsigns to state using lookup on hamqth.com. script will need to be updated to use your hamqth.com. credentials. if callsign doesnt exist on hamqth. take the states it outputs and put into a file called "states.txt". I usually keep a running "states.txt" file and update it to add states after doing an activation. if callsign doesnt exist on hamqth, it says not found and i manually look it up (qrz.com seems to be more complete these days, that would be a nice upgrade for this script).

usstateCompleteCheck.py

this script takes the "states.txt" file created in the previous step and checks what states have not been contacted. outputs results to screen

parksTODOgps.py

Awards



Bronze Activator



Silver Activator



Gold Activator



Platinum Activator



Bronze Hunter



Silver Hunter



Gold Hunter



Platinum Hunter



Diamond Hunter



Sapphire Hunter



Arizona Agave



Enrubio Hunter



Ouachita Mountain Goldenrod Hunter



Park to Park



RaDAR-Warthog



RaDAR-Rhino



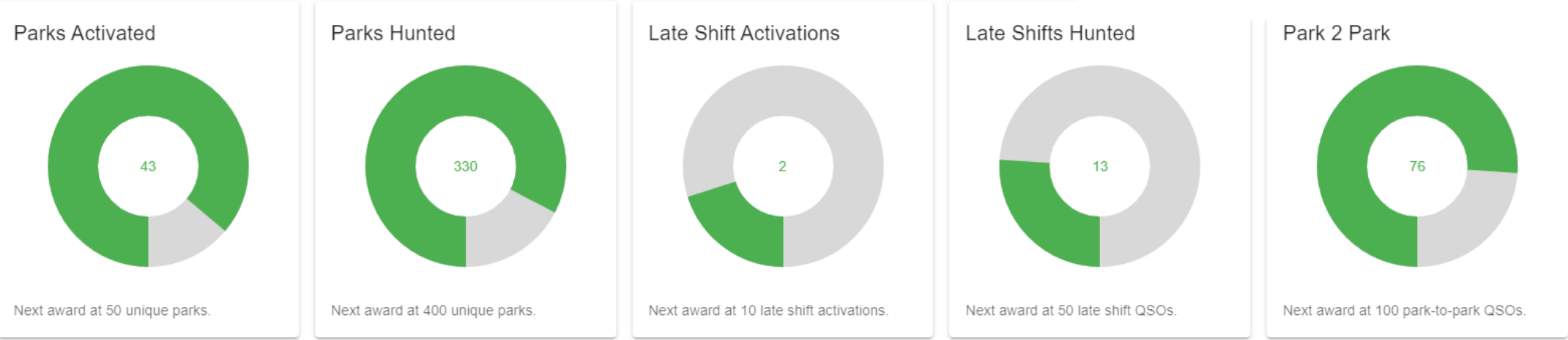
RaDAR-Cheetah



RaDAR-Ostrich

All-Time Statistics

	Activator	Hunter
Activations	46 / 46	----
Parks	43 / 43	330
QSOs	1123 / 1123	430



Activated US States

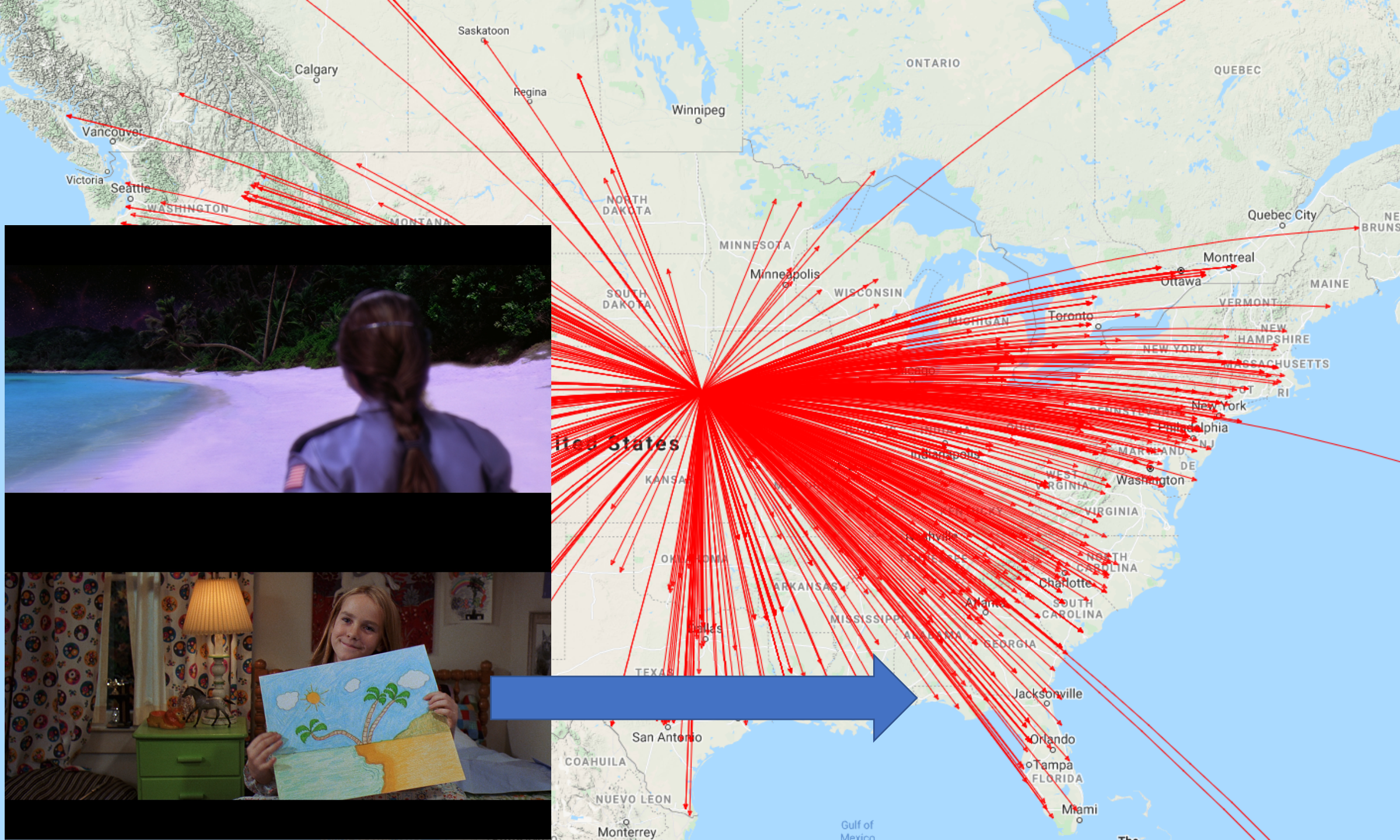
AK	AL	AR	AZ	CA	CO	CT	DC	DE	FL	GA	HI	IA	ID	IL	IN	KS	KY	LA	MA	MD
ME	MI	MN	MO	MS	MT	NC	ND	NE	NH	NJ	NM	NV	NY	OH	OK	OR	PA	RI	SC	SD
TN	TX	UT	VA	VT	WA	WI	WV	WY												

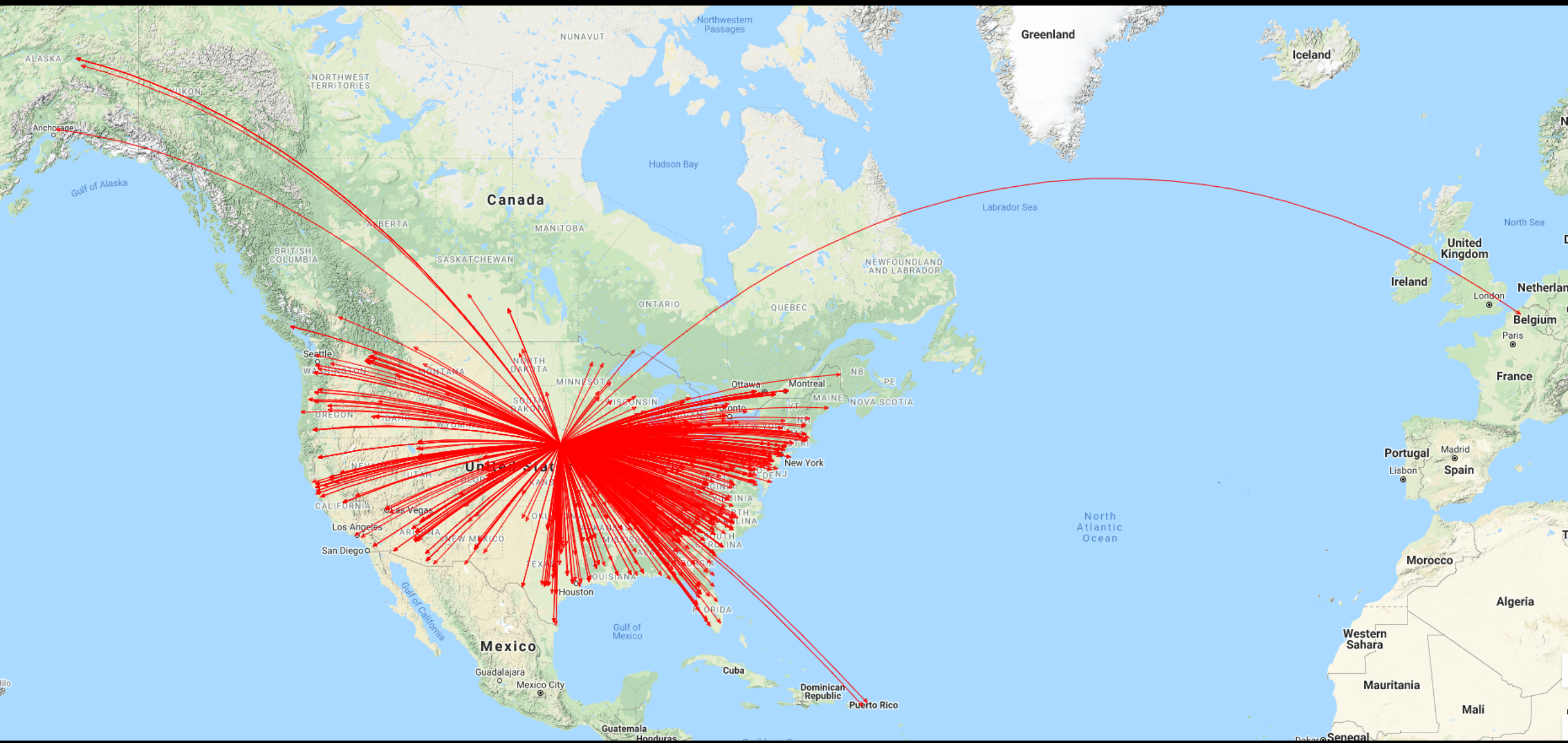
Activate a park in 50 states (DC is a wildcard) to earn this award.

Hunted US States

AK	AL	AR	AZ	CA	CO	CT	DC	DE	FL	GA	HI	IA	ID	IL	IN	KS	KY	LA	MA	MD
ME	MI	MN	MO	MS	MT	NC	ND	NE	NH	NJ	NM	NV	NY	OH	OK	OR	PA	RI	SC	SD
TN	TX	UT	VA	VT	WA	WI	WV	WY												

Hunt a park in 50 states (DC is a wildcard) to earn this award.





Some things I liked along the way

- QSL cards
- ISS contact
- SSTV



Thanks!

- There is a looooooooooot more to talk about, but hopefully you got a taste!
- zonksec – Tyler Rosonke