Hack the Stars

Yacko, Wacko, and Dot
animaniacs2k20@gmail.com

How did I get here? Is this talk for me?

This talk is about where “the enterprise” intersects space.

Do you have IT?

Do you have remote sites that use VSATs?

What about field deployed IoT devices using short burst messaging systems?

Do you have boats?

Do you have a satellite?

Do you pentest groups with any of the above?

Who Are We?

We deliver pentesting and security engineering support to numerous telecommunications clients around the world, and Dot is actively involved in the operation of an RF-sensing cubesat.

We regularly compete in the WCTF, and can be found near piles of Pelican cases loaded with antennas and blinking lights.

Ground Rules For This Talk:

Keeping this as approachable as possible.

Highlighting the work of individuals that made this easy for you.

Demonstrating how accessible the space segment really is.

Empowering skiddies with dangerous knowledge to drive industrial change.

Questions to Answer Today:

Level Set Part 1: How did this whole SATCOM thing grow up?

Level Set Part 2: What are the components in a modern SATCOM scenario?

Inspire Fear: What are some basic attacks any skid can employ?

Shopping List: How can an individual gear up to learn?

Empower with Tools: What are some steps my shop can take today to dip our toes in our space segment?

Other Work

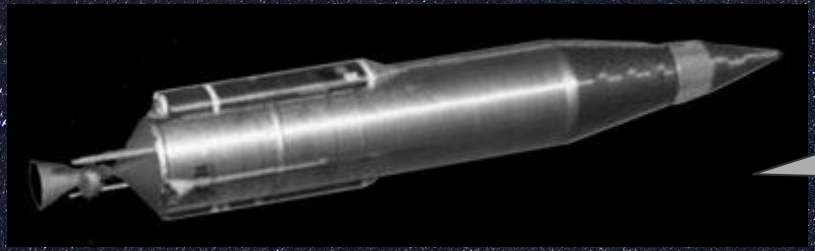
Satcom presentation from IWSSC 2008 - Lloyd Wood
https://savi.sourceforge.io/about/lloyd-wood-iwssc-08-tutorial.pdf

DEF CON 23 - Colby Moore

https://www.slideshare.net/Synack/spread-spectrum-satcom-hacking-attacking-the-globalstar-simplex-data-service

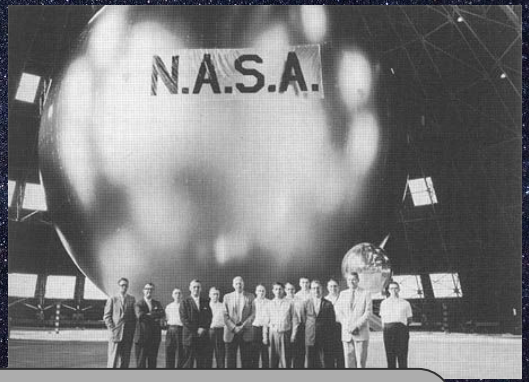
Level Set: Part 1

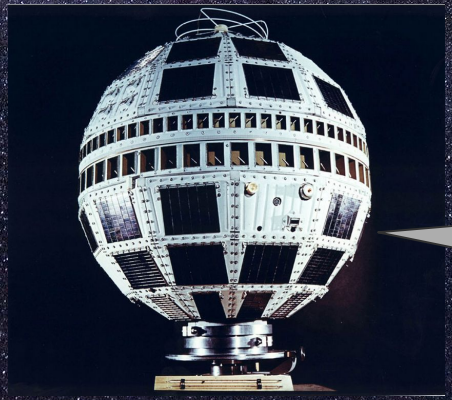
How did this whole SATCOM thing grow up?



SCORE (1958 - 62 Years Ago)
Shortwave transmission of a recorded tape on orbit

Echo 1 (1960 - 60 Years Ago)
Basically a giant inflatable reflector; bounces microwaves across the earth





Telstar 1 (1962 - 58 Years Ago)
The first “transponder” on orbit.

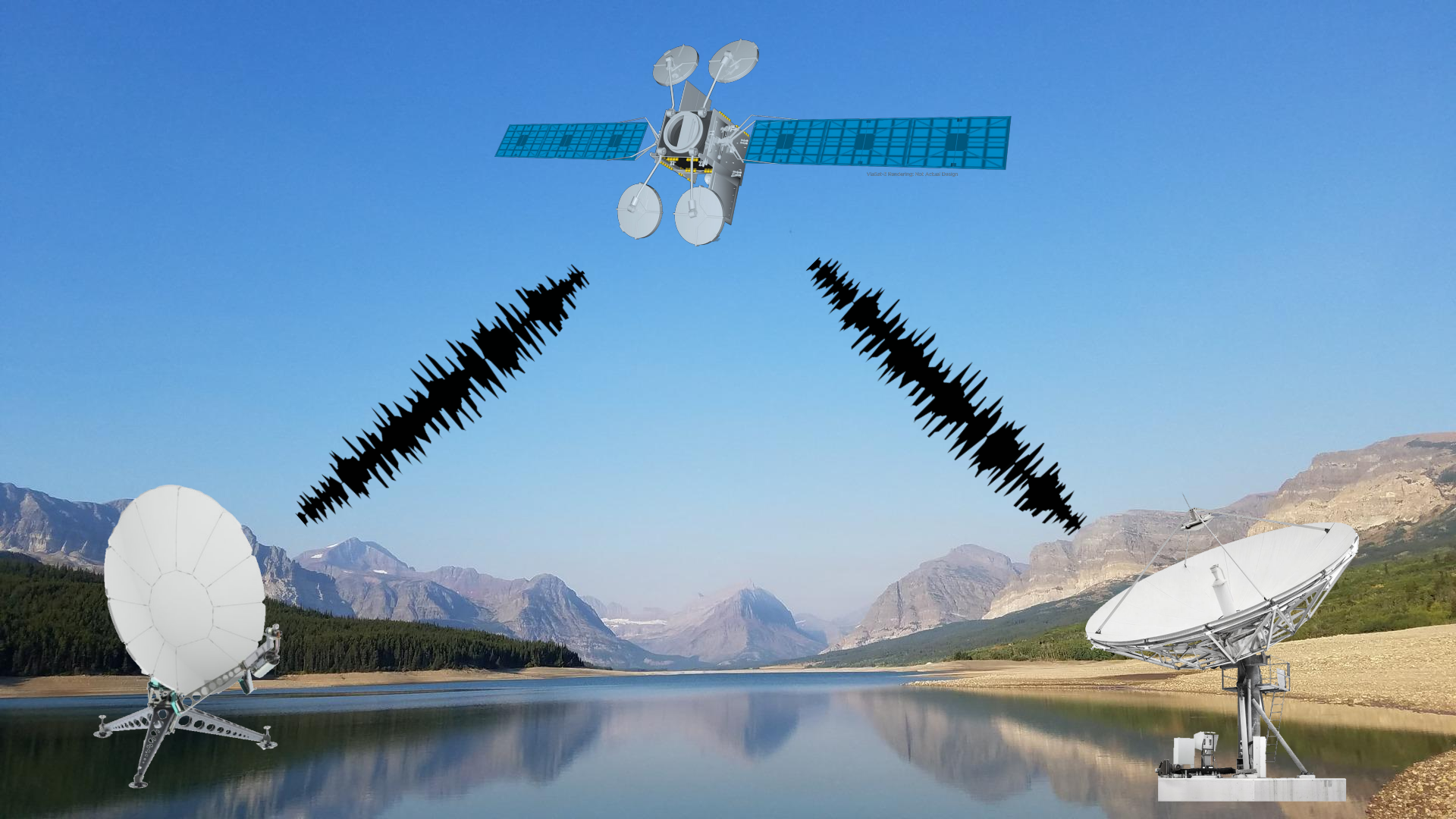

iridium
Everywhere
HawkEye 360
INTELSAT
Viasat
HughesNet
SES
Globalstar
planet.

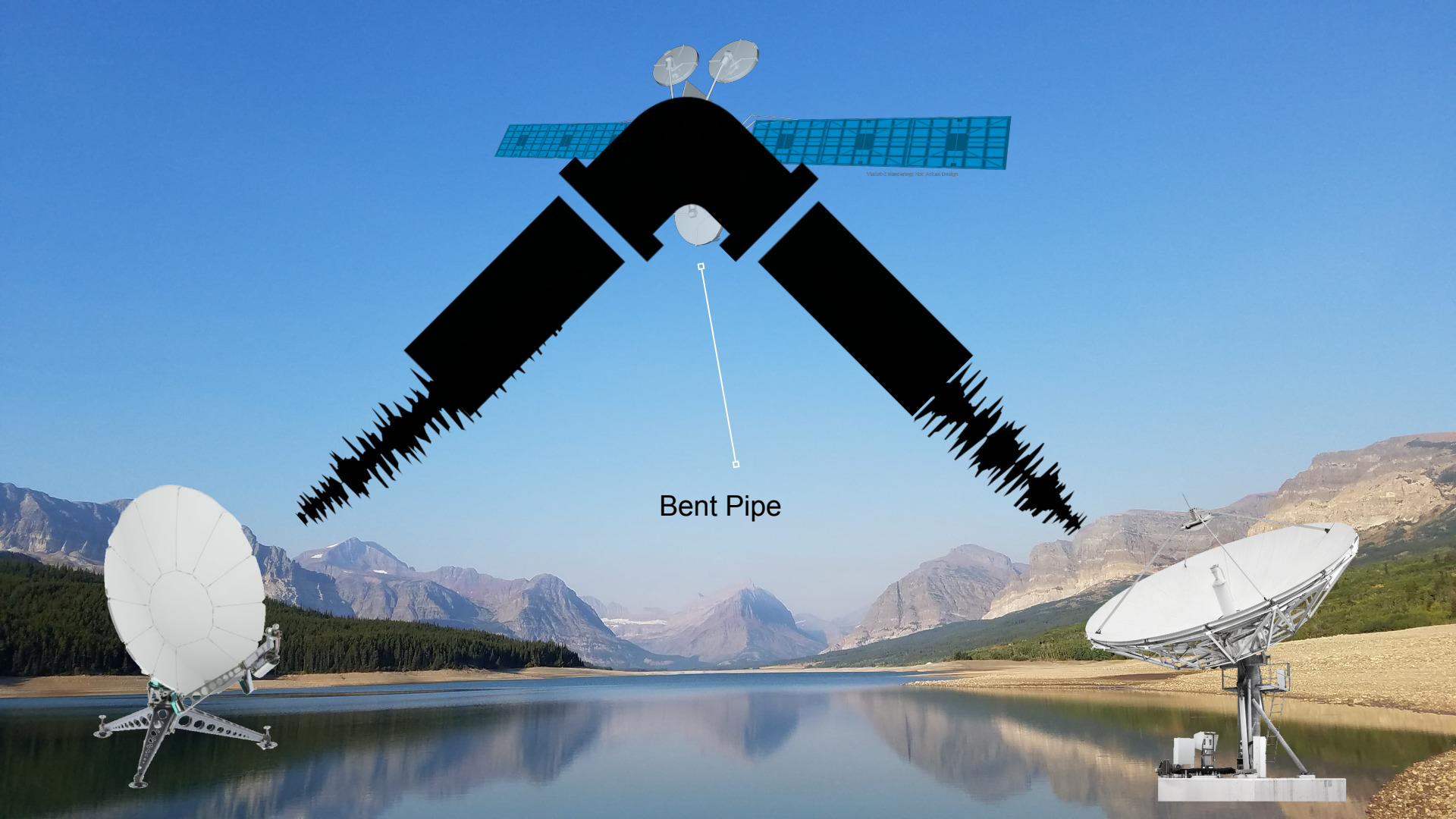
Level Set: Part 2

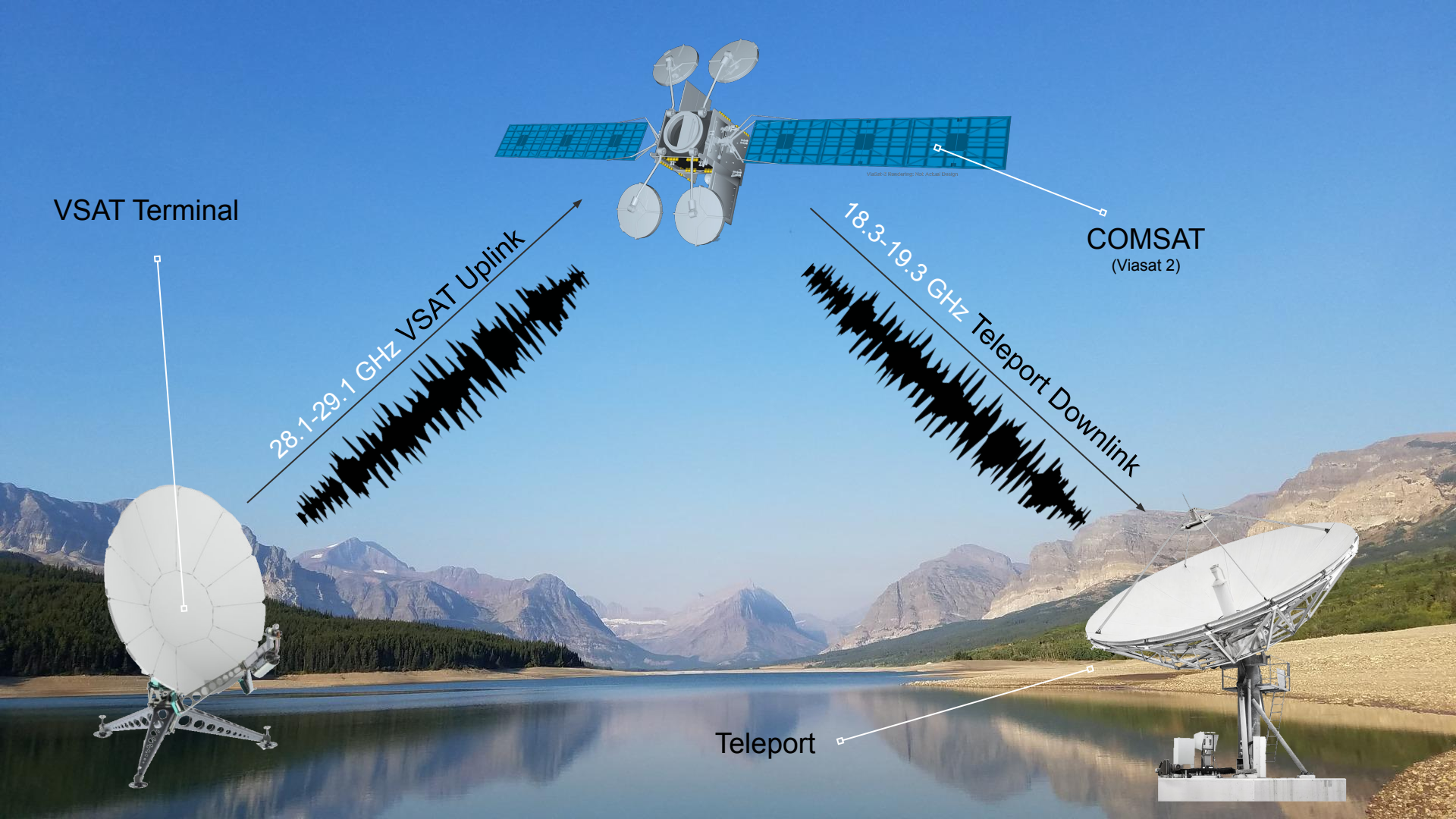
What are the components in a modern SATCOM scenario?

Standard Radar Frequency Letter-Band Nomenclature(IEEE Standard 521-2002)

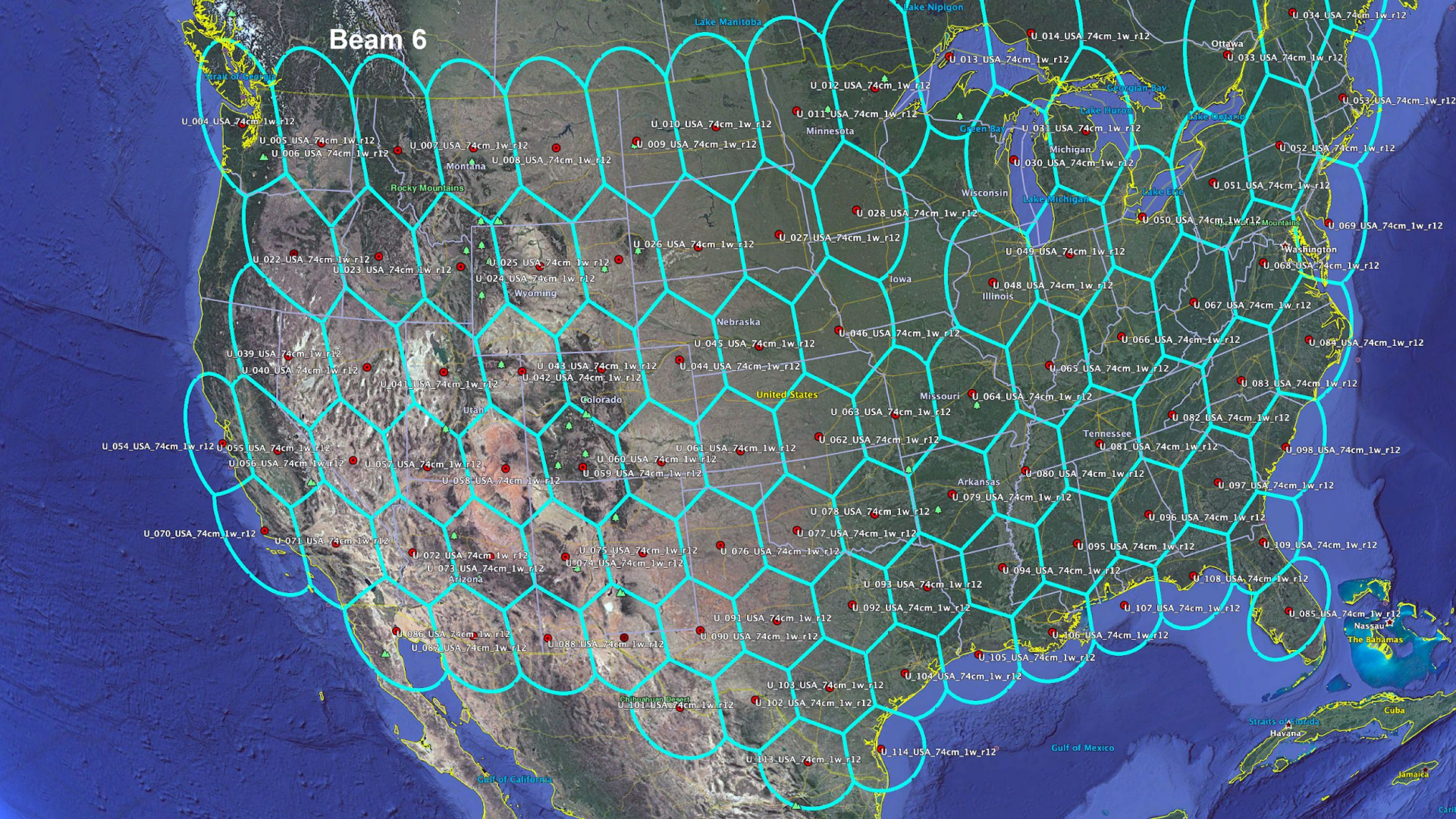
Band Designator	Frequency (GHz)	Wavelength in Free Space (centimeters)
HF	0.003 to 0.030	10000 to 1000
VHF	0.030 to 0.300	1000 to 100
UHF	0.300 to 1	100 to 30.0
L band	1 to 2	30.0 to 15.0
S band	2 to 4	15 to 7.5
C band	4 to 8	7.5 to 3.8
X band	8 to 12	3.8 to 2.5
Ku band	12 to 18	2.5 to 1.7
K band	18 to 27	1.7 to 1.1
Ka band	27 to 40	1.1 to 0.75
V band	40 to 75	0.75 to 0.40
W band	75 to 110	0.40 to 0.27
mm	110 to 300	0.27 to 0.10

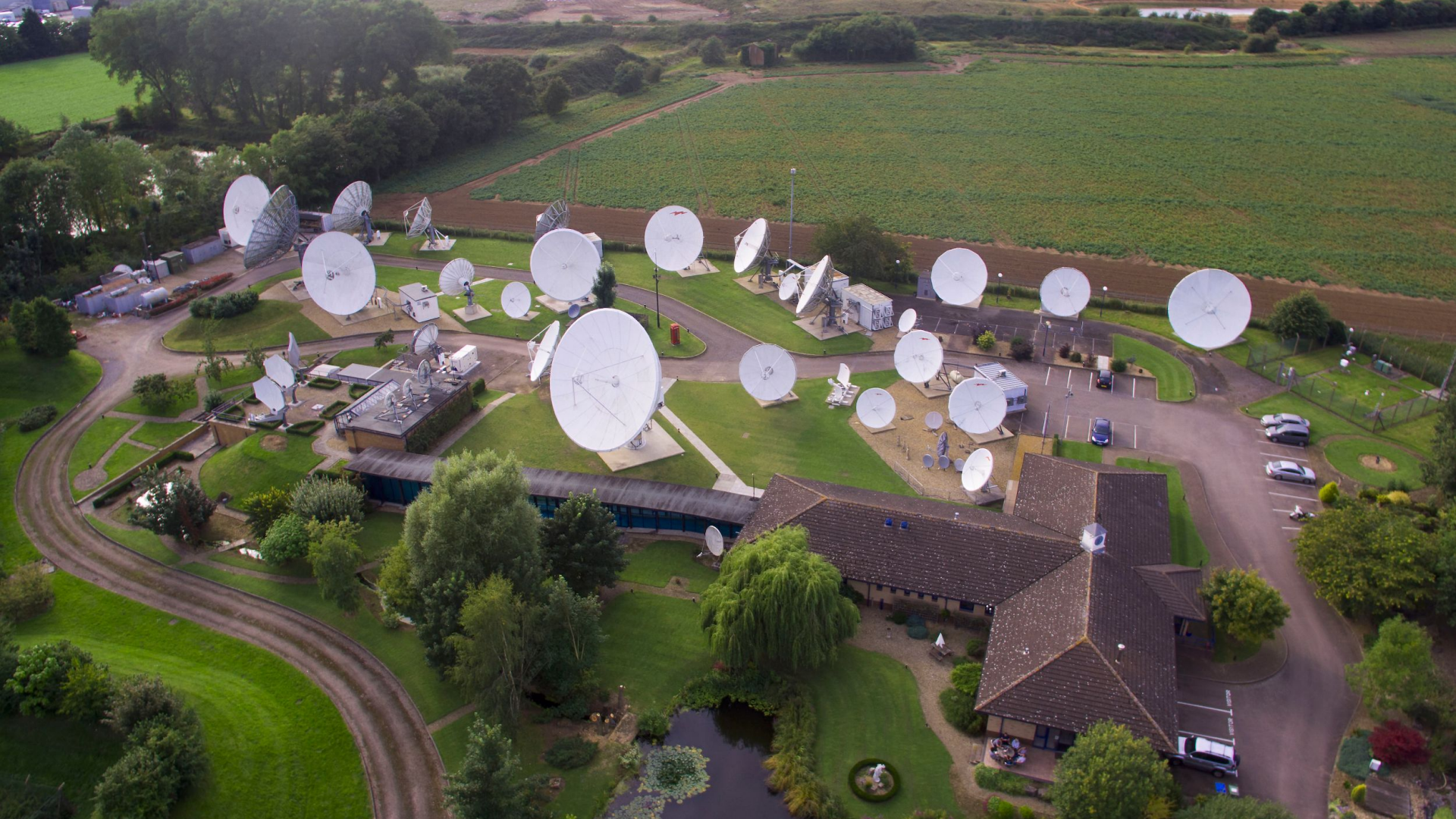

Visualized Rendering, Not Actual Design

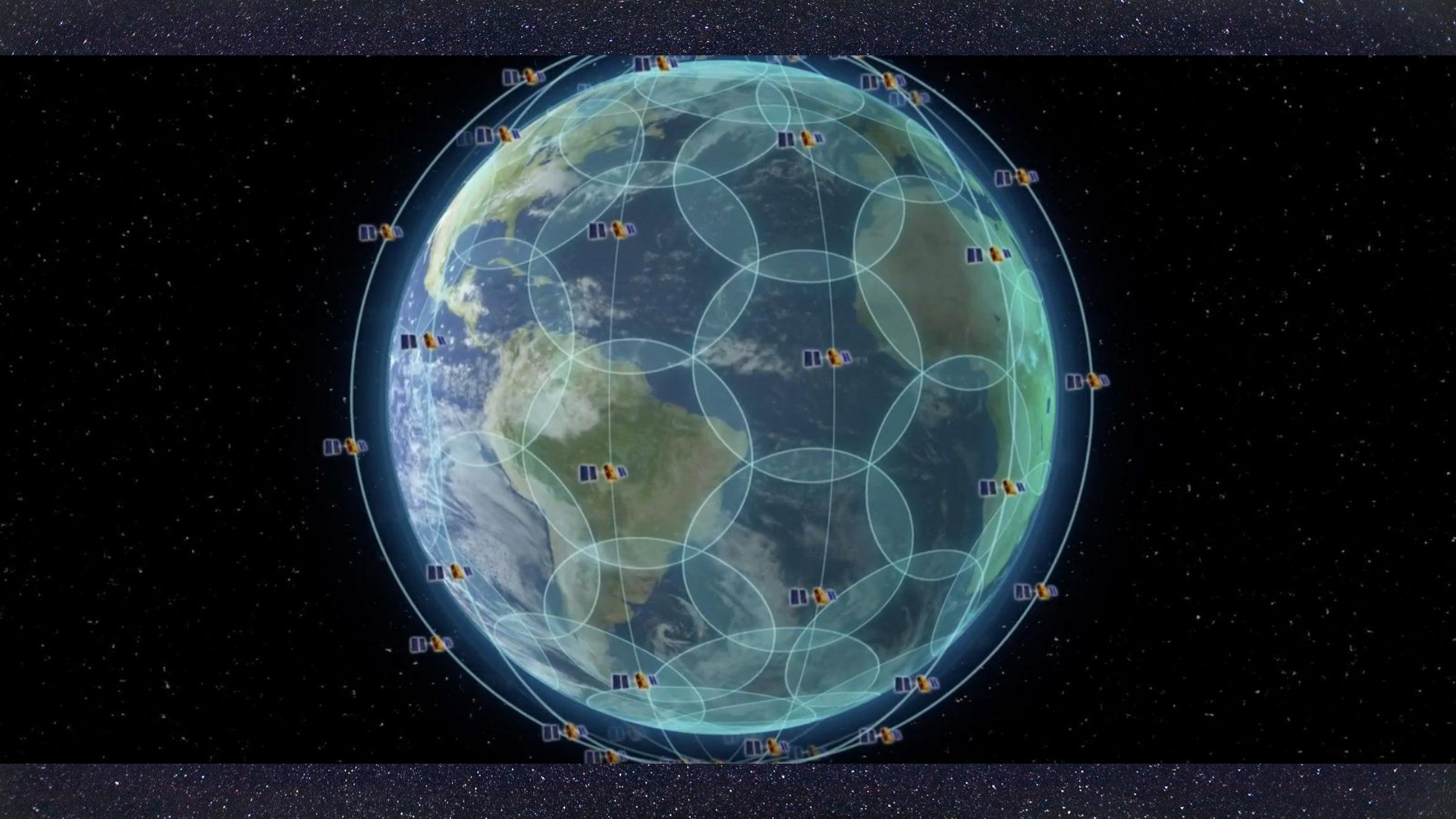

Bent Pipe


VSAT Terminal
28.1-29.1 GHz VSAT Uplink
18.3-19.3 GHz Teleport Downlink
COMSAT
(Viasat 2)
Teleport


RigNet


Beam 6
Lake Manitoba
Lake Nipigon
Ottawa
Georgian Bay
Lake Huron
Lake Ontario
Green Bay
Minnesota
Michigan
Wisconsin
Lake Michigan
Lake Erie
Montana
Rocky Mountains
Wyoming
Iowa
Illinois
Nebraska
Colorado
Utah
Missouri
United States
Tennessee
Arkansas
Arizona
Washington
Appalachian Mountains
Nassau
The Bahamas
Cuba
Havana
Straits of Florida
Gulf of Mexico
Jamaica
Gulf of California
Chihuahuan Desert
U_004_USA_74cm_1w_r12
U_005_USA_74cm_1w_r12
U_006_USA_74cm_1w_r12
U_007_USA_74cm_1w_r12
U_008_USA_74cm_1w_r12
U_009_USA_74cm_1w_r12
U_010_USA_74cm_1w_r12
U_011_USA_74cm_1w_r12
U_012_USA_74cm_1w_r12
U_013_USA_74cm_1w_r12
U_014_USA_74cm_1w_r12
U_022_USA_74cm_1w_r12
U_023_USA_74cm_1w_r12
U_024_USA_74cm_1w_r12
U_025_USA_74cm_1w_r12
U_026_USA_74cm_1w_r12
U_027_USA_74cm_1w_r12
U_028_USA_74cm_1w_r12
U_030_USA_74cm_1w_r12
U_031_USA_74cm_1w_r12
U_033_USA_74cm_1w_r12
U_034_USA_74cm_1w_r12
U_039_USA_74cm_1w_r12
U_040_USA_74cm_1w_r12
U_041_USA_74cm_1w_r12
U_042_USA_74cm_1w_r12
U_043_USA_74cm_1w_r12
U_044_USA_74cm_1w_r12
U_045_USA_74cm_1w_r12
U_046_USA_74cm_1w_r12
U_048_USA_74cm_1w_r12
U_049_USA_74cm_1w_r12
U_050_USA_74cm_1w_r12
U_051_USA_74cm_1w_r12
U_052_USA_74cm_1w_r12
U_053_USA_74cm_1w_r12
U_054_USA_74cm_1w_r12
U_055_USA_74cm_1w_r12
U_056_USA_74cm_1w_r12
U_057_USA_74cm_1w_r12
U_058_USA_74cm_1w_r12
U_059_USA_74cm_1w_r12
U_060_USA_74cm_1w_r12
U_061_USA_74cm_1w_r12
U_062_USA_74cm_1w_r12
U_063_USA_74cm_1w_r12
U_064_USA_74cm_1w_r12
U_065_USA_74cm_1w_r12
U_066_USA_74cm_1w_r12
U_067_USA_74cm_1w_r12
U_068_USA_74cm_1w_r12
U_069_USA_74cm_1w_r12
U_070_USA_74cm_1w_r12
U_071_USA_74cm_1w_r12
U_072_USA_74cm_1w_r12
U_073_USA_74cm_1w_r12
U_074_USA_74cm_1w_r12
U_075_USA_74cm_1w_r12
U_076_USA_74cm_1w_r12
U_077_USA_74cm_1w_r12
U_078_USA_74cm_1w_r12
U_079_USA_74cm_1w_r12
U_080_USA_74cm_1w_r12
U_081_USA_74cm_1w_r12
U_082_USA_74cm_1w_r12
U_083_USA_74cm_1w_r12
U_084_USA_74cm_1w_r12
U_085_USA_74cm_1w_r12
U_086_USA_74cm_1w_r12
U_087_USA_74cm_1w_r12
U_088_USA_74cm_1w_r12
U_090_USA_74cm_1w_r12
U_091_USA_74cm_1w_r12
U_092_USA_74cm_1w_r12
U_093_USA_74cm_1w_r12
U_094_USA_74cm_1w_r12
U_095_USA_74cm_1w_r12
U_096_USA_74cm_1w_r12
U_097_USA_74cm_1w_r12
U_098_USA_74cm_1w_r12
U_101_USA_74cm_1w_r12
U_102_USA_74cm_1w_r12
U_103_USA_74cm_1w_r12
U_104_USA_74cm_1w_r12
U_105_USA_74cm_1w_r12
U_106_USA_74cm_1w_r12
U_107_USA_74cm_1w_r12
U_108_USA_74cm_1w_r12
U_109_USA_74cm_1w_r12
U_113_USA_74cm_1w_r12
U_114_USA_74cm_1w_r12






Iridium 2
iridium
10:45
iridium


IRIDIUM COMMUNICATIONS, INC
SBD9602E
SN: J0011O
WARRANTY
VOID IF
BROKEN

RockBLOCK Mk2 - Iridium SatComm Module

WRL-13745 ROHS ★★★★½ 16

$249.95

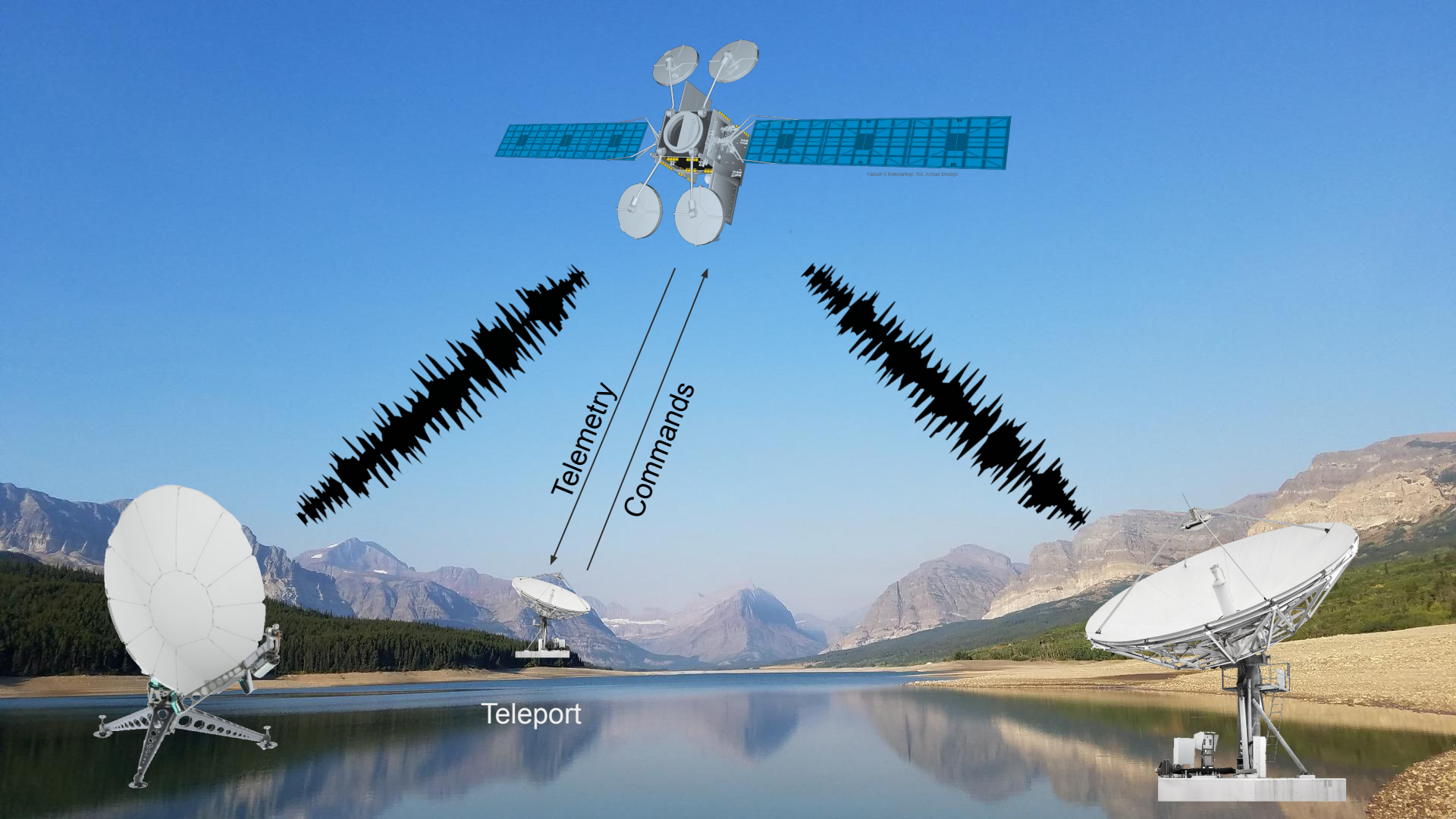
Shipping outside of the US?
Click here for info

- 1 + ADD TO CART

Stock availability

DESCRIPTION FEATURES DOCUMENTS

The RockBLOCK Mk2 allows you to send and receive short messages from anywhere on Earth with a clear view of the sky and it works far beyond the reach of WiFi and GSM networks. Maybe you


Telemetry
Commands
Teleport

Inspire Fear

What are some basic attacks any skid can employ?

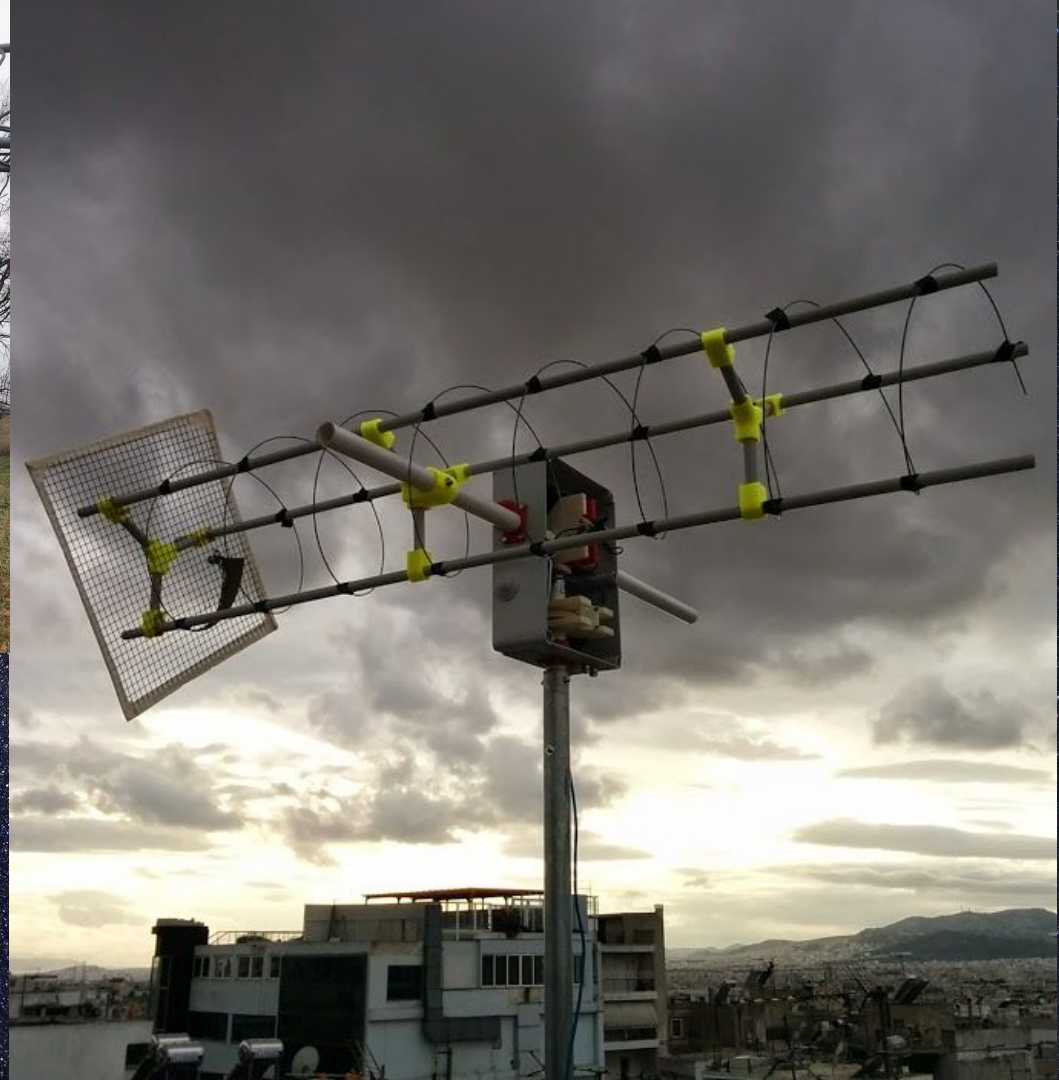
Brazilians on the US Navy Fleet Satellites
https://www.wired.com/2009/04/fleetcom/


FBI
10:01 41°
FOX 45
SCAMMERS USING FOIL
WAYNESVILLE


peplink
Balance30
EATON

https://www.ab9il.net/wlan-projects/wifi6.html

ILLINOIS
Aerospace Engineering
GRAINGER COLLEGE OF ENGINEERING



Shopping List

How can an individual gear up to learn?

What's my target?

First, ID a bird and a buzz:

http://www.ne.jp/asahi/hamradio/je9pel/satslist.htm

Second, figure out where to point:

https://www.n2yo.com/satellite/

What Do I Do With a TLE?

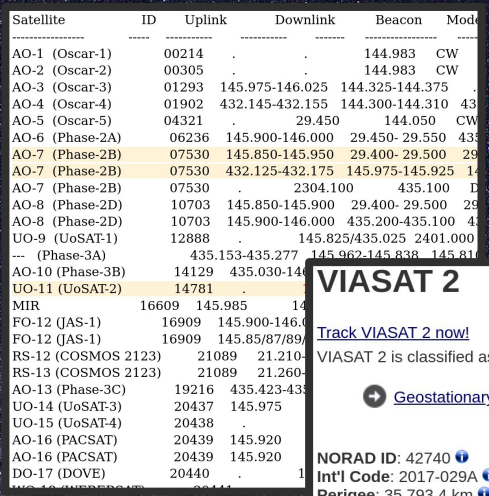
1 42740U 17029A 20030.03174373 -.00000263 00000-0 00000+0 0 9990
2 42740 0.0076 261.2885 0000055 128.3883 40.5494 1.00272329 9828

Write some python and use Skyfield!

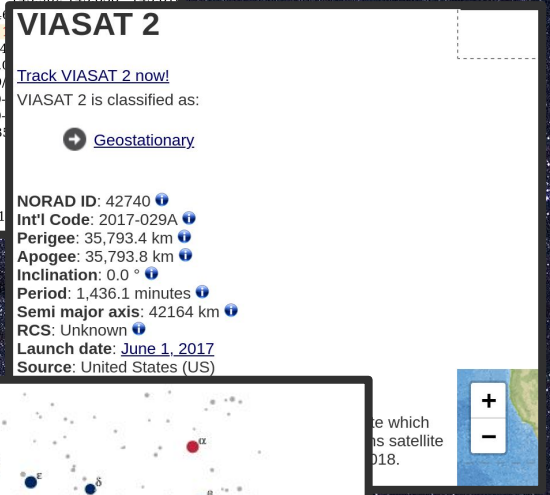
https://rhodesmill.org/skyfield/

***Do you have infinite money? If so, check out AGI's toolset:

https://www.agi.com/home



Satellite	ID	Uplink	Downlink	Beacon	Mode
AO-1 (Oscar-1)	00214	.	.	144.983	CW
AO-2 (Oscar-2)	00305	.	.	144.983	CW
AO-3 (Oscar-3)	01293	145.975-146.025	144.325-144.375	.	
AO-4 (Oscar-4)	01902	432.145-432.155	144.300-144.310	43	
AO-5 (Oscar-5)	04321	.	29.450	144.050	CW
AO-6 (Phase-2A)	06236	145.900-146.000	29.450- 29.550	43	
AO-7 (Phase-2B)	07530	145.850-145.950	29.400- 29.500	29	
AO-7 (Phase-2B)	07530	432.125-432.175	145.975-145.925	14	
AO-7 (Phase-2B)	07530	.	2304.100	435.100	D
AO-8 (Phase-2D)	10703	145.850-145.900	29.400- 29.500	29	
AO-8 (Phase-2D)	10703	145.900-146.000	435.200-435.100	43	
UO-9 (UoSAT-1)	12888	.	145.825/435.025	2401.000	
--- (Phase-3A)		435.153-435.277	145.962-145.838	145.81	
AO-10 (Phase-3B)	14129	435.030-146			
UO-11 (UoSAT-2)	14781	.			
MIR	16609	145.985	14		
FO-12 (JAS-1)	16909	145.900-146.0			
FO-12 (JAS-1)	16909	145.85/87/89/			
RS-12 (COSMOS 2123)	21089	21.210-			
RS-13 (COSMOS 2123)	21089	21.260-			
AO-13 (Phase-3C)	19216	435.423-43			
UO-14 (UoSAT-3)	20437	145.975			
UO-15 (UoSAT-4)	20438	.			
AO-16 (PACSAT)	20439	145.920			
AO-16 (PACSAT)	20439	145.920			
DO-17 (DOVE)	20440	.	1		



VIASAT 2

Track VIASAT 2 now!

VIASAT 2 is classified as:

Geostationary

NORAD ID: 42740
Int'l Code: 2017-029A
Perigee: 35,793.4 km
Apogee: 35,793.8 km
Inclination: 0.0 °
Period: 1,436.1 minutes
Semi major axis: 42164 km
RCS: Unknown
Launch date: June 1, 2017
Source: United States (US)

e which
s satellite
018.

VHF through C Band

Antenna - https://www.wa5vjb.com/ Log Periodics are cheap and easy for receiving beacon signals. $33 for 400MHz to 1GHz, $20 for 850MHz to 6.5GHz

LNA - https://www.nooelec.com/store/lana.html goes 20MHz - 4GHz “ok” - $29.95

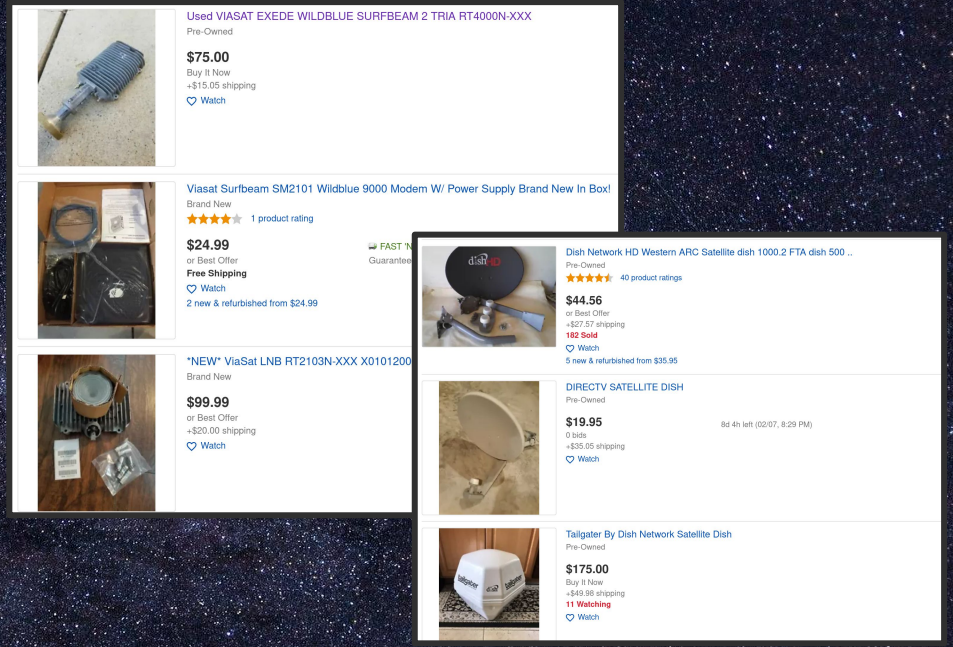
Radio - https://www.nooelec.com/store/sdr/nesdr-smart-sdr.html This RTL-SDR will power the LNA and work for a lot of beacon discovery on the lower bands. $23.95
Or go the hackRF route: https://greatscottgadgets.com/hackrf/one/ which goes DC to 6GHz for about $330

Computer - Raspberry Pi 4 currently $41.98 on Amazon

And with all that… you can follow this tutorial:
https://www.raspberrypi.org/blog/build-a-satnogs-ground-station-raspberry-pi-3b-hackspace-magazine-18/

C Band and Beyond!

1) Pick a target
2) Hit eBay (or Craigslist, LetItGo, Facebook Marketplace, etc)
3) Start doing that OSINT. Hint: look for words like “vsat buc” if you want to transmit, or “LNB” for receive.
4) Most of these items are designed to convert the satellite signal down to L-band! Slap that feed on a 2nd hand dish, hook it up to your SDR and get pointing!



Software for this SDR thing?

GNURadio - Simultaneously the most approachable and unapproachable SDR software in the world! Don't worry, there are some easy buttons.
https://www.gnuradio.org/

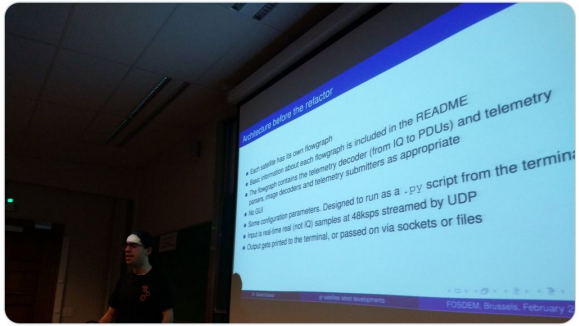
gr-satellites - Family of "Out of Tree (OOT)" modules for GNURadio to get you quickly demoding and decoding satellite data.
https://github.com/daniestevez/gr-satellites
https://destevez.net/

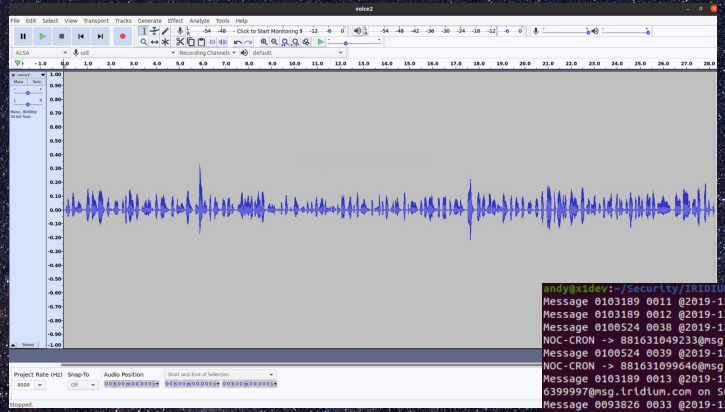
Note: Your package manager probably uses a dated version of gr-3.7. gr-3.8 broke a bunch of dated api functions, and a lot of out of tree modules take some work to compile. The next couple months may be a tough time to get in to gnuradio. PyBombs is a great community tool, but as of February 2, 2020- you'll save a lot of headache by reading directions carefully and building up your toolchain from source.

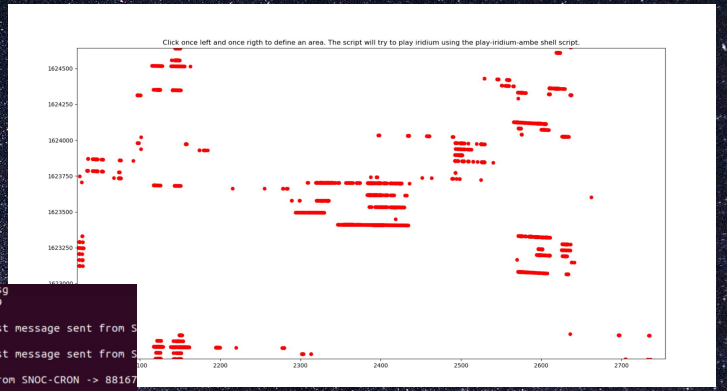
GNURadio
THE FREE & OPEN SOFTWARE RADIO ECOSYSTEM

Fresh Hot Take!

Marcus Müller @dEnergy_dTime · 4h
Daniel @ea4gpz presents gr-satellites at #FOSDEM2020 and h… approached the maintainability problem of a module having MASSIVE amounts of decoder.
He's come up with a yaml-based DSL!
github.com/daniestevez/gr…








```
andy@xidev:~/Security/IRIDIUM/extractions$ reassembler.py -i output.parsed -m msg
Message 0103189 0011 @2019-12-22T12:37:57 (len:0) 111 OK  : 1736Z GM-bo 12222019
Message 0103189 0012 @2019-12-22T12:38:07 (len:0)  69 OK  : 173636
Message 0100524 0038 @2019-12-22T13:16:27 (len:1)  54 OK  : nm@smtp.iwcs.net Test message sent from S
NOC-CRON -> 881631049233@msg.iridium.com on Sun Dec 22 18:15:02 GMT 2019
Message 0100524 0039 @2019-12-22T13:16:29 (len:1)  41 OK  : nm@smtp.iwcs.net Test message sent from S
NOC-CRON -> 881631099646@msg.iridium.com on Sun Dec 22 18:15:02 GMT 2019
Message 0103189 0013 @2019-12-22T13:16:51 (len:1) 108 OK  : Test message sent from SNOC-CRON -> 88167
6399997@msg.iridium.com on Sun Dec 22 18:15:02 GMT 2019
Message 0093826 0033 @2019-12-22T13:19:00 (len:1)  40 OK  : nm@smtp.iwcs.net Test message sent from S
NOC-CRON -> 881631099656@msg.iridium.com on Sun Dec 22 18:15:02 GMT 2019
Message 0103189 0014 @2019-12-22T13:36:17 (len:0) 111 OK  : 1826Z GM-bo 12222019
Message 0103189 0015 @2019-12-22T13:36:22 (len:0)  68 OK  : 182727
Message 3525461 0061 @2019-12-22T13:53:56 (len:0) 110 OK  : page #1
Message 3525461 0062 @2019-12-22T14:00:21 (len:0) 109 OK  : page #2
Message 0093826 0034 @2019-12-22T14:17:16 (len:1)  39 OK  : nm@smtp.iwcs.net Test message sent from S
NOC-CRON -> 881631099656@msg.iridium.com on Sun Dec 22 19:15:02 GMT 2019
Message 0100524 0040 @2019-12-22T14:17:59 (len:1)  40 OK  : nm@smtp.iwcs.net Test message sent from S
NOC-CRON -> 881631099646@msg.iridium.com on Sun Dec 22 19:15:02 GMT 2019
Message 0100524 0041 @2019-12-22T14:18:00 (len:1)  53 OK  : nm@smtp.iwcs.net Test message sent from S
NOC-CRON -> 881631049233@msg.iridium.com on Sun Dec 22 19:15:02 GMT 2019
Message 0103189 0016 @2019-12-22T14:18:22 (len:1) 107 OK  : Test message sent from SNOC-CRON -> 88167
6399997@msg.iridium.com on Sun Dec 22 19:15:02 GMT 2019
Message 0103189 0017 @2019-12-22T14:28:07 (len:0) 110 OK  : 1926Z GM-bo 12222019
Message 0103189 0018 @2019-12-22T14:28:17 (len:0)  71 OK  : 192525
Message 0100524 0042 @2019-12-22T15:16:19 (len:1)  49 OK  : nm@smtp.iwcs.net Test message sent from S
NOC-CRON -> 881631099646@msg.iridium.com on Sun Dec 22 20:15:01 GMT 2019
Message 0100524 0043 @2019-12-22T15:16:27 (len:1)  62 OK  : nm@smtp.iwcs.net Test message sent from S
NOC-CRON -> 881631049233@msg.iridium.com on Sun Dec 22 20:15:01 GMT 2019
Message 0094297 0034 @2019-12-22T15:16:41 (len:2)  43 fail: supervisor@northerncom.com ==========000
0003159==============[MISSING]= 3159 - Lac Seul For:Leeane Capay P
Message 0103189 0019 @2019-12-22T15:16:42 (len:1) 116 OK  : Test message sent from SNOC-CRON -> 88167
6399997@msg.iridium.com on Sun Dec 22 20:15:01 GMT 2019
Message 3525461 0063 @2019-12-22T15:18:09 (len:0) 108 OK  : page #3
Message 0093826 0035 @2019-12-22T15:18:51 (len:1)  48 OK  : nm@smtp.iwcs.net Test message sent from S
NOC-CRON -> 881631099656@msg.iridium.com on Sun Dec 22 20:15:01 GMT 2019
Message 3525461 0064 @2019-12-22T15:21:24 (len:0) 107 OK  : page #4
Message 3525461 0065 @2019-12-22T15:27:50 (len:0) 106 OK  : page #5
Message 0103189 0020 @2019-12-22T15:36:07 (len:0)  85 OK  : 203131
Message 0103189 0062 @2019-12-22T15:36:10 (len:0)  15 OK  : 881676390000
Message 0103189 0083 @2019-12-22T15:36:19 (len:0) 122 OK  : 2031Z GM-bo 12222019
Message 0103189 0082 @2019-12-22T15:36:25 (len:0)  85 OK  : 203131
Message 0094297 0035 @2019-12-22T15:52:22 (len:2)  38 fail: supervisor@northerncom.com ==========000
0003159================ Sun 22-Dec-19 02:44p ********************************[MISSING]
```

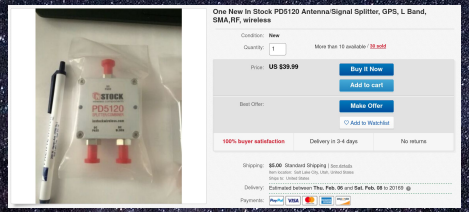
gr-iridium

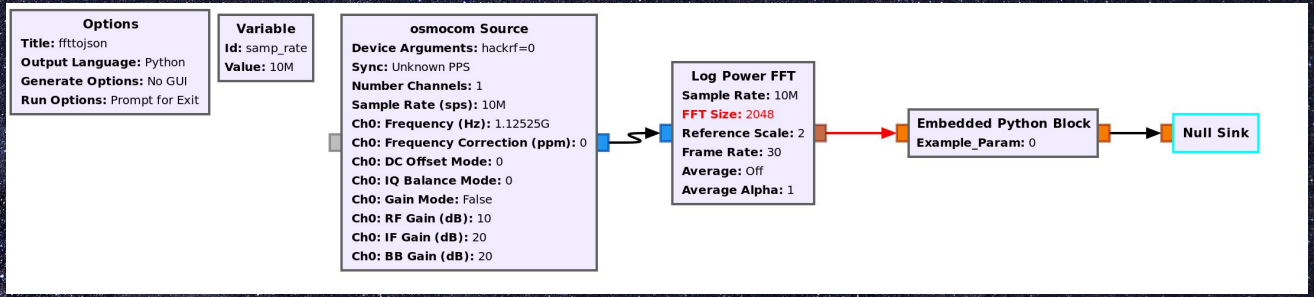
https://github.com/muccc/gr-iridium

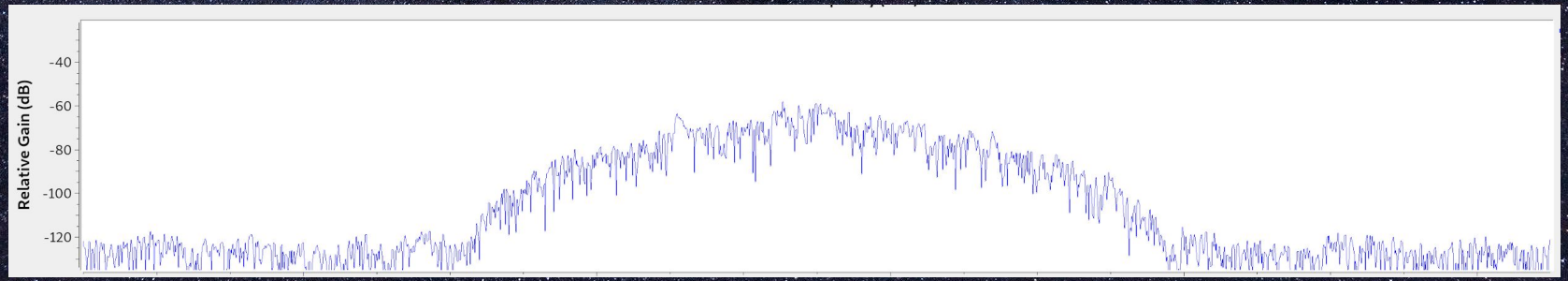
Empower with Tools

What are some steps my shop can take?

Instrument Your L-Band VSAT

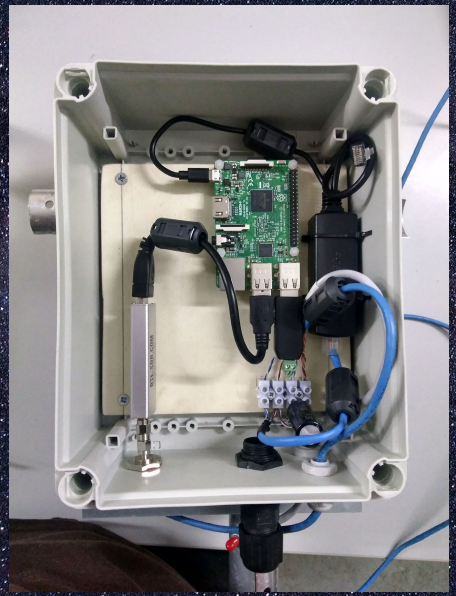






Set up a SatNOGS Station

https://wiki.satnogs.org/Get_Started



Road Getting Longer

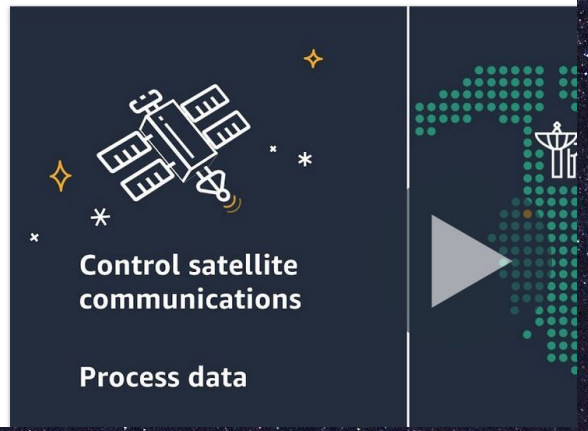
What’s coming next to keep making this complicated?

AWS Ground Station

Easily control satellites and ingest data with fully managed Ground Station as a Service

Get Started

AWS Ground Station is a fully managed service that lets you control satellite communications, process data, and scale your operations without having to worry about building or managing your own ground station infrastructure. Satellites are used for a wide variety of use cases, including weather forecasting, surface imaging, communications, and video broadcasts. Ground stations form the core of global satellite networks. With AWS Ground Station, you have direct access to AWS services and the AWS Global Infrastructure including a low-latency global fiber network. For example, you can use Amazon S3 to store the downloaded data, Amazon Kinesis Data Streams for managing data ingestion from satellites, Amazon SageMaker for building custom machine learning applications that apply to your data sets. You can save up to 80% on the cost of your ground station operations



References

Transponder definitions with citation needed https://en.wikipedia.org/wiki/Transponder_%28satellite_communications%29
Sky pic https://pixnio.com/media/horizon-lake-panorama-reflection-mountain
Definitions and bent pipe overview https://www.britannica.com/technology/satellite-communication/How-satellites-work
Viasat 2 image https://www.viasat.com/sites/default/files/media/images/viasat_3_rendering.png
Teleport dish http://www.teliportglobal.com/
Litesat 2.2 pic http://www.litecoms.com/litesat_2-2-2/
Carrier wave https://pixabay.com/vectors/audio-music-sfa-jazz-sound-wave-1293262/
Viasat freqs https://www.tbs-satellite.com/tse/online/sat_viasat_1.html https://www.ofcom.org.uk/__data/assets/pdf_file/0037/49879/viasat.pdf
Vsat picture https://www.mobilsat.com/Fixed-satellite-internet/Hardware/Dishes-Mountains.png
Rignet picture https://www.offshore-technology.com/wp-content/uploads/sites/6/2017/09/deck.jpg
Intelsat teleport http://www.intelsat.com/global-network/intelsatone/teleports/
Po-lice picture https://www.mobilsat.com/VSAT/US-Govt.jpg
Teleport image https://io-sat.com/wp-content/uploads/2017/11/DJI_0016.jpg
Spot beams https://rvseniormoments.files.wordpress.com/2019/08/02_hughesnet-gen-5-spot-beams.jpg
Iridium go https://satavenue.se/wp-content/uploads/2017/03/Iridium-GO_1.jpg
Rockblock https://i1.wp.com/cdn.makezine.com/uploads/2014/01/m37-rockblock1_edited_large.jpg
Iridium constellation https://thumbs-prod.si-cdn.com/a1qfIX-X5W40lVKo1UXp2FmCoCc=/fit-in/1600x0/filters:focal(1178x560:1179x561)/https://public-media.si-cdn.com/filer/19/e8/19e89559-6694-4340-98d5-f3a266e70e21/14h_ij2019_iridium_next_live.jpg
Screenshot https://www.sparkfun.com/products/13745
Modem in a rack https://www.vsat-shop.com/intellian-v60ka-band-vsat-antenna-lease
Wifi yagi https://www.ab9il.net/wlan-projects/wifi6.html
Satnogs website (projects) https://satnogs.org/documentation/projects/
Teleport image https://www.romsenter.no/var/ezdemo_site/storage/images/media/images/industri-bedrifter-teknologiutveksling/telenor/telenor-teleport/68361-1-nor-NO/Telenor-teleport.jpg
U of I satellite launch https://aerospace.illinois.edu/news/student-cubesail-satellite-launch-imminent
Bent pipe https://ya-webdesign.com/editor.html?id=2825998
Score https://space.skyrocket.de/doc_sdat/score.htm
Echo 1 https://en.wikipedia.org/wiki/Project_Echo
Telestar https://www.space.com/16549-telstar-satellite-first-tv-signal-anniversary.html
Planet Logo https://commons.wikimedia.org/wiki/File:Planet_Labs_logo.svg