HACK THE … HEMISPHERË!!!



Karl Koscher (@supersat)
Andrew Green



Tweets 893 | Following 41 | Followers 1,505 | Likes 29

Following

Shadytel

@shadytel Follows you

Some people play Fantasy Football. We play Fantasy Phone Company. RT & Follow may imply endorsement. May not be legal in all jurisdictions. Use as directed.

Shady Cove, OR, USA

shady.tel

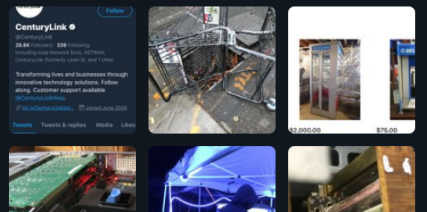
Joined June 2010

Tweet to | Message

118 Followers you know



47 Photos and videos

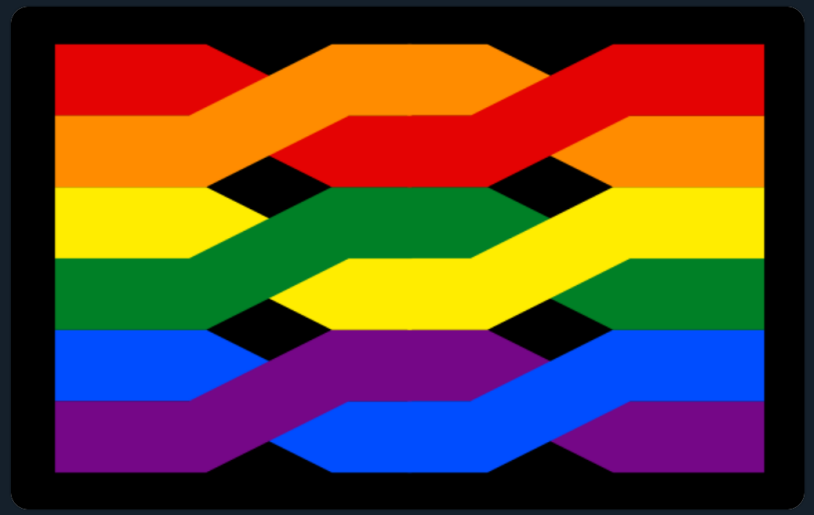


Tweets | Tweets & replies | Media

Pinned Tweet

Shadytel @shadytel · 28 Jun 2015

#pride2015 #billingexcellence #twistedpride



3 | 32 | 87

Shadytel @shadytel · Mar 31

Celebrate this Trans Day of Visibility with us! We're giving a 10% discount to everyone whose gender is null in the database. Also we're giving one lucky nonbinary customer free line rental this month: Daves Bread! Congratulations, Daves!

11 | 40

Who to follow · Refresh · View all

#abolish(pol)ICE @banasi... Follow

Matthew Garrett @mjg59 Follow

franklin @TheDevilsVoice Follow

Find people you know
Import your contacts from Gmail

Connect other address books

Worldwide trends · Change

Giants
316K Tweets

#NFLDraft
305K Tweets

Haskins
137K Tweets

#TaylorSwiftTONIGHT
83.8K Tweets

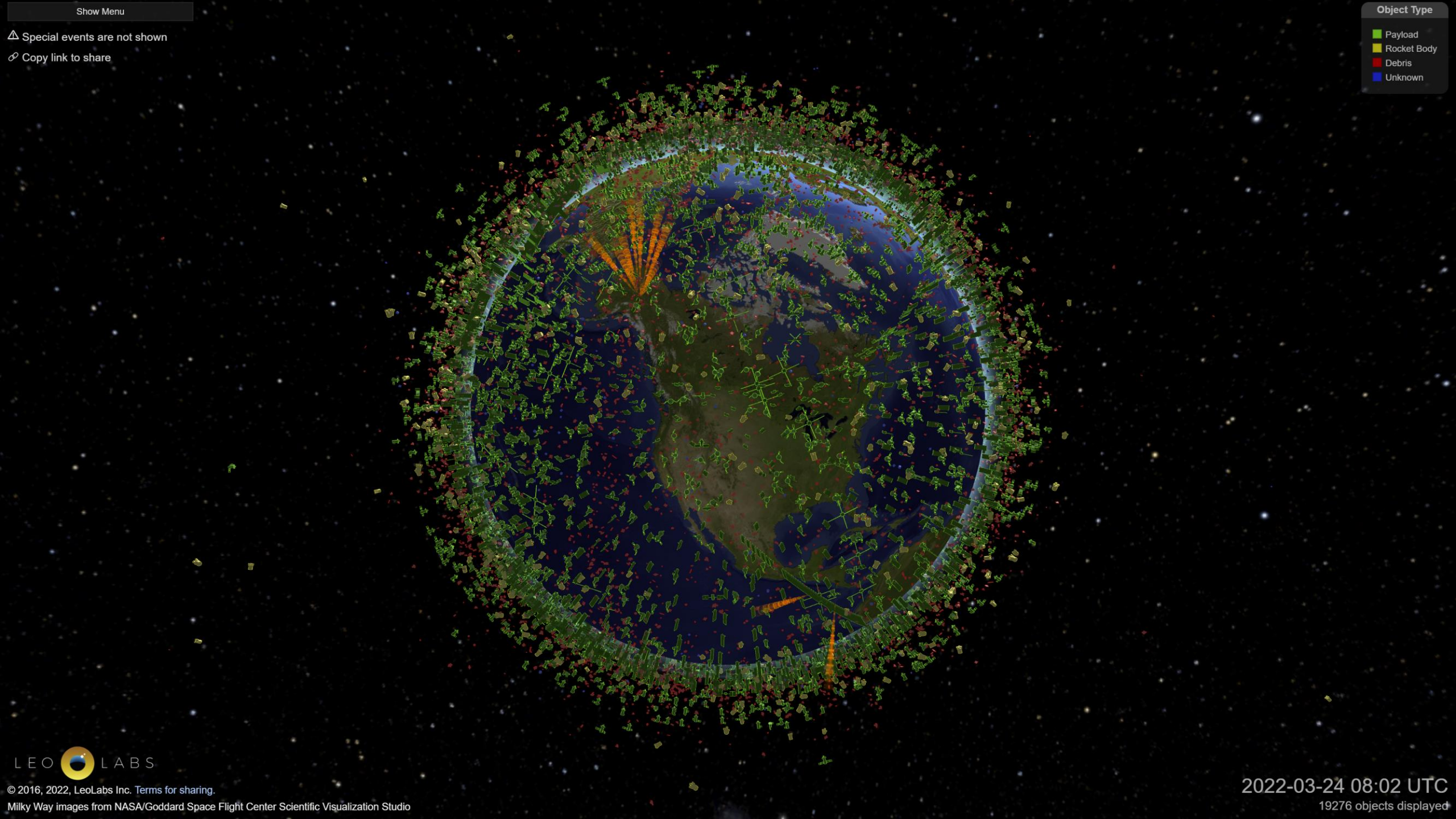
Raiders
119K Tweets



39
ShadyTel Phone Directory
As of July 11 at 1am

3002 CO ISDN
3101 Staff
3099 Free ShadyCamp
3333 the LOL
3210 Duncan's Hamock
3102 Staff Camp
3216 RV Franklin Hu
3999 Annc cct
3133 T Prophet
3995 Cabins DSI Drop
3825 Nick F
3826 Milliways
3003 Black Lodge 1
3004 Black Lodge 2
3005 Garret (Ada's)
3232 Ada's
3323 Alex
3007 PDX
3008 Noisebridge 1
3009 Noisebridge 2
3012 Hak5
3011 Leviathan
3217 RF pal
3323 Alex
3021 Cabin 9
3022 Hack Casual
3023 Registration
3667 DoorPhone
3013 NinjaTel 1
3014 NinjaTel 2
3024 Deprogram
3015 Anything
3016 Nick Lewis (Nerd Creation Lab)
3411 TC Info Desk
3337 Caesar
3020 Neg9




Show Menu
Special events are not shown
Copy link to share
Object Type
Payload
Rocket Body
Debris
Unknown
LEO LABS
© 2016, 2022, LeoLabs Inc. Terms for sharing.
Milky Way images from NASA/Goddard Space Flight Center Scientific Visualization Studio
2022-03-24 08:02 UTC
19276 objects displayed

LEO/MEO Satellite Deficiencies

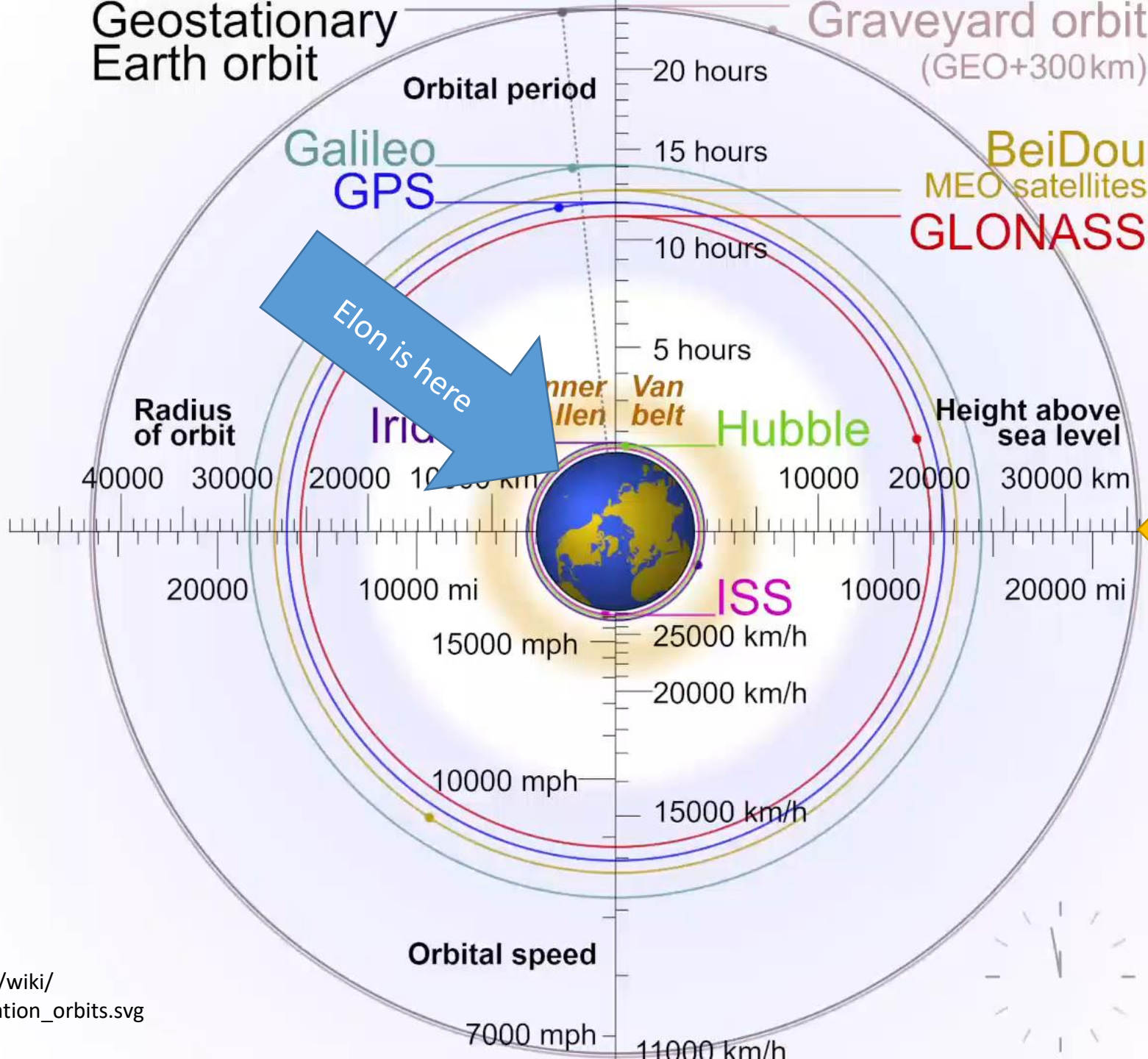
- **Broadcast dishes are aimed at a fix point in the sky**
  - **Greatly simplifies installation, maintenance, lifespan, etc.**
- **LEO/MEO satellites require *constellations* for continuous coverage**
  - **GPS requires 24**
  - **Starlink requires THOUSANDS**



© 2022 Northwestern Telephone and Telegraph
PROPRIETARY AND CONFIDENTIAL



© 2022 Northwestern Telephone and Telegraph
PROPRIETARY AND CONFIDENTIAL



We are here

https://commons.wikimedia.org/wiki/File:Comparison_satellite_navigation_orbits.svg
By cmglee. CC BY-SA 3.0.

Satellite Lifecycles

- **Satellites have limited lifespans**
  - **Limited fuel for fine-tuning orbit/position**
  - **Batteries wear out**
  - **Space debris**
  - **Radiation**
- **Satellites are engineered for a specified lifespan**
- **Geosynchronous satellites moved to “graveyard orbit” at EOL**
  - **Minimize risk of space debris**
  - **Requires far less fuel than deorbiting**

© 2022 Northwestern Telephone and Telegraph
PROPRIETARY AND CONFIDENTIAL

An Unprecedented Opportunity…

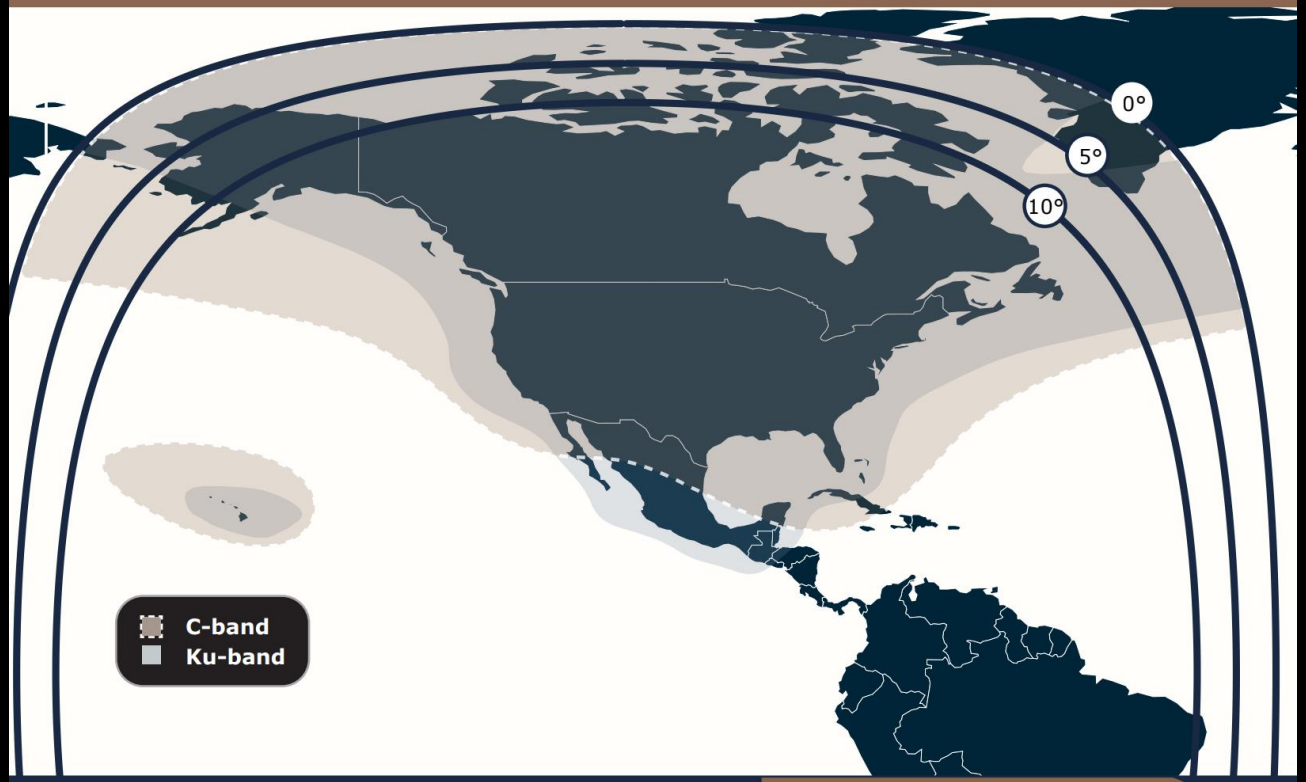


© 2022 Northwestern Telephone and Telegraph
PROPRIETARY AND CONFIDENTIAL

Anik F1R

Strong North American coverage
in C- and Ku-band frequencies





- Ideal for video distribution to cable systems and for broadcast contribution
- Coverage of all 50 United States and Canada including the Far North
- Flexibility to support virtually any application

Key Facts

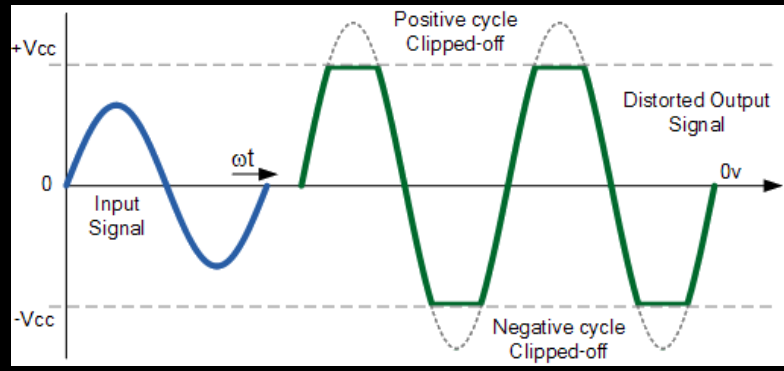
SATELLITE MANUFACTURER
Airbus Defence and Space

TRANSPONDERS
24 C-band @ 36MHz
32 Ku-band @ 27MHz

IN SERVICE DATE
October 2005

Satellite Transponders

- **Dumb “bent pipes”**
  - **Receives/bandpass filters uplink signals**
  - **Translates frequencies to downlink band**
  - **Linearly amplifies/bandpass filters downlink signal**
- **Any RF signal received is retransmitted as-is!**
  - **Not tied to any particular modulation scheme**
  - **No authentication either 😅**
- **Multiple uplinks can share a transponder**
  - **Power levels must be approximately the same**

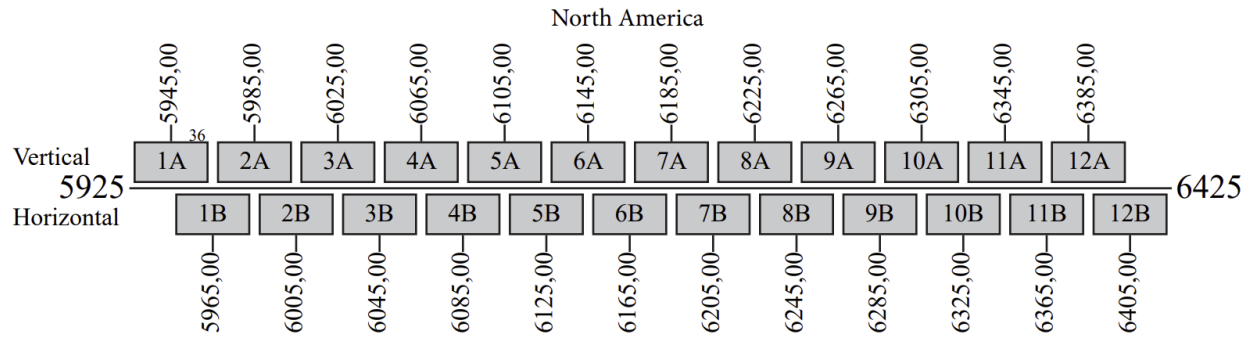


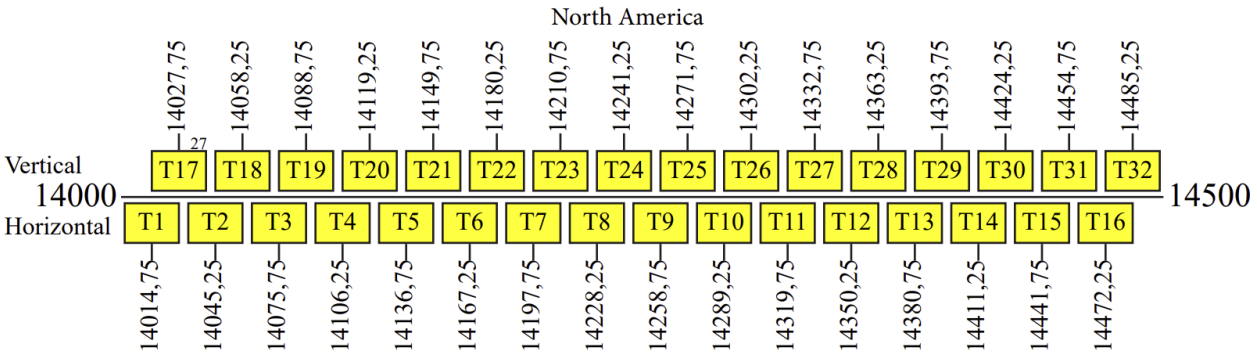
BENT PIPE URL
https://www.electronics-tutorials.ws/

© 2022 Northwestern Telephone and Telegraph
PROPRIETARY AND CONFIDENTIAL

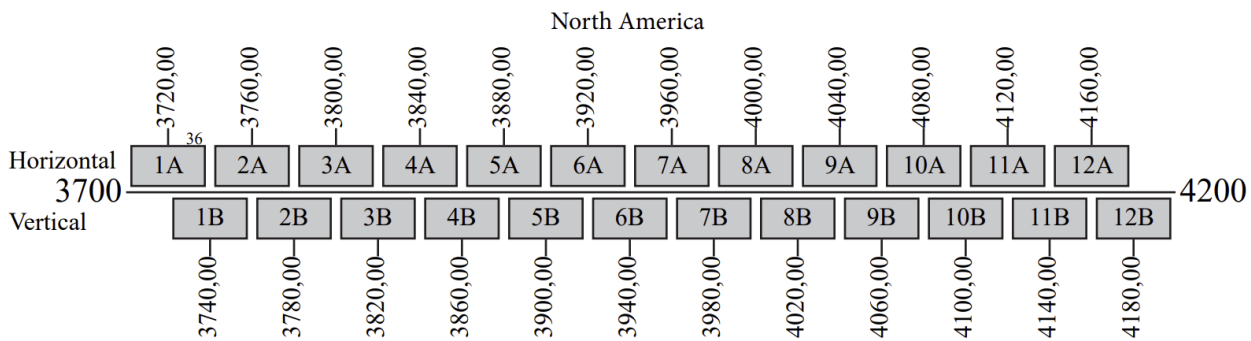
Anik F1R Transponder Configuration

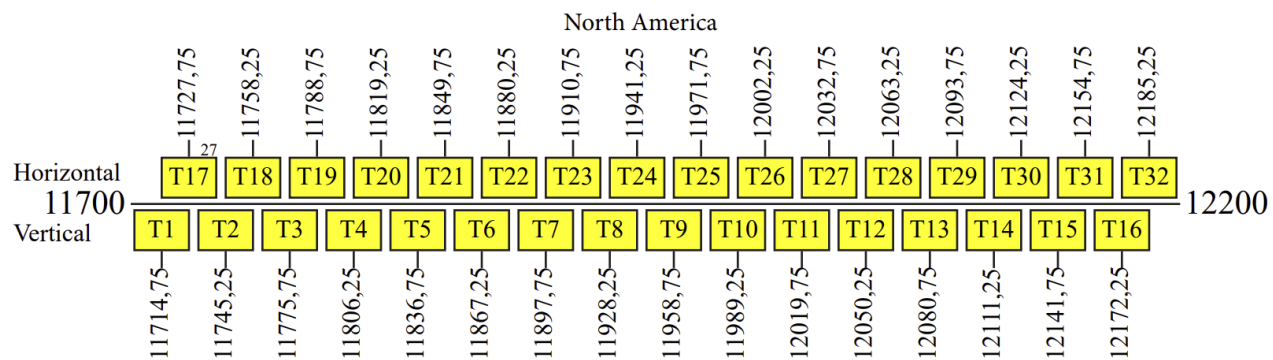
Uplink





Downlink





© 2022 Northwestern Telephone and Telegraph
PROPRIETARY AND CONFIDENTIAL

http://frequencyplansatellites.altervista.org/Telesat/Anik_F1R.pdf

Our Uplink



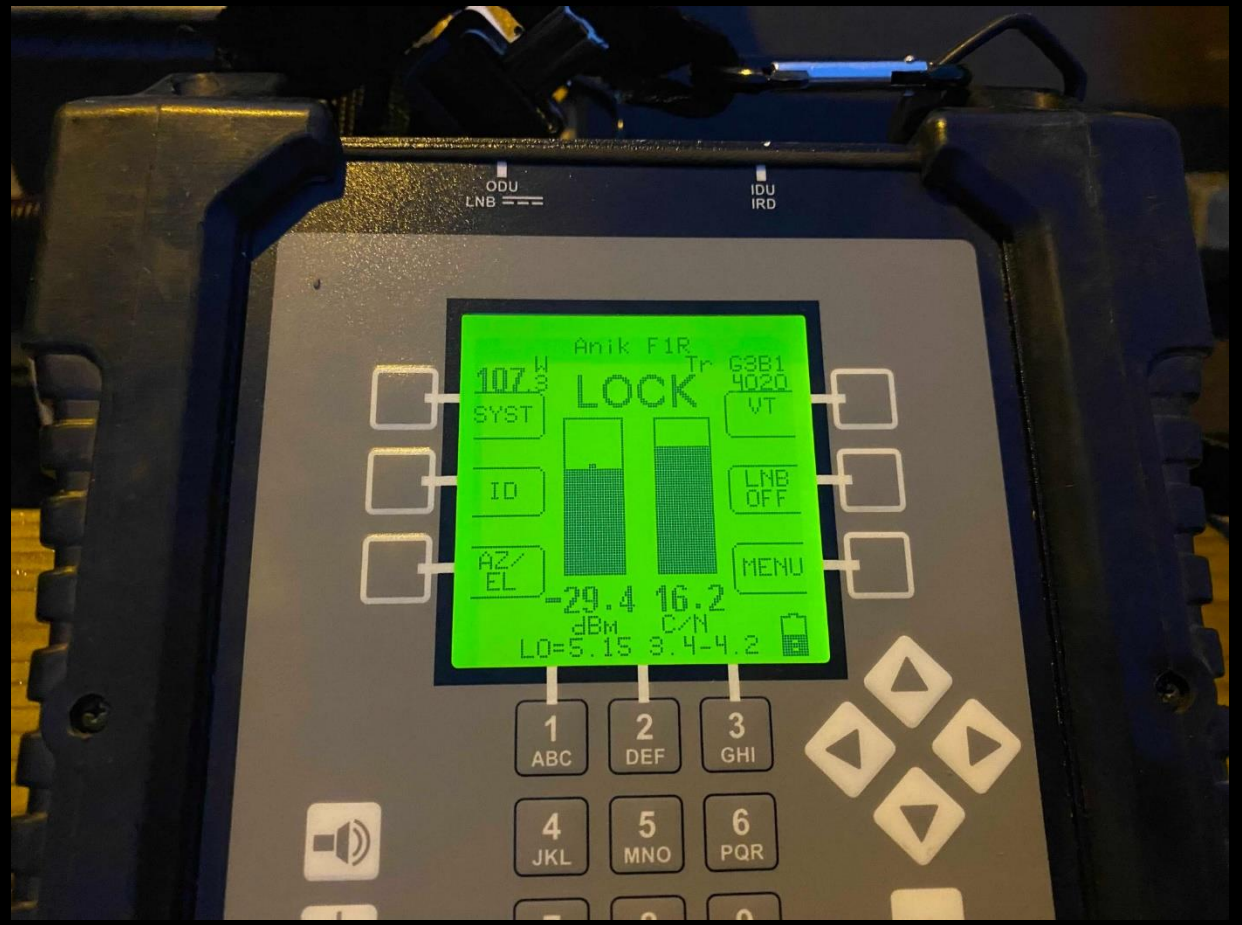
© 2022 Northwestern Telephone and Telegraph
PROPRIETARY AND CONFIDENTIAL

Our Uplink



© 2022 Northwestern Telephone and Telegraph
PROPRIETARY AND CONFIDENTIAL

Our Uplink



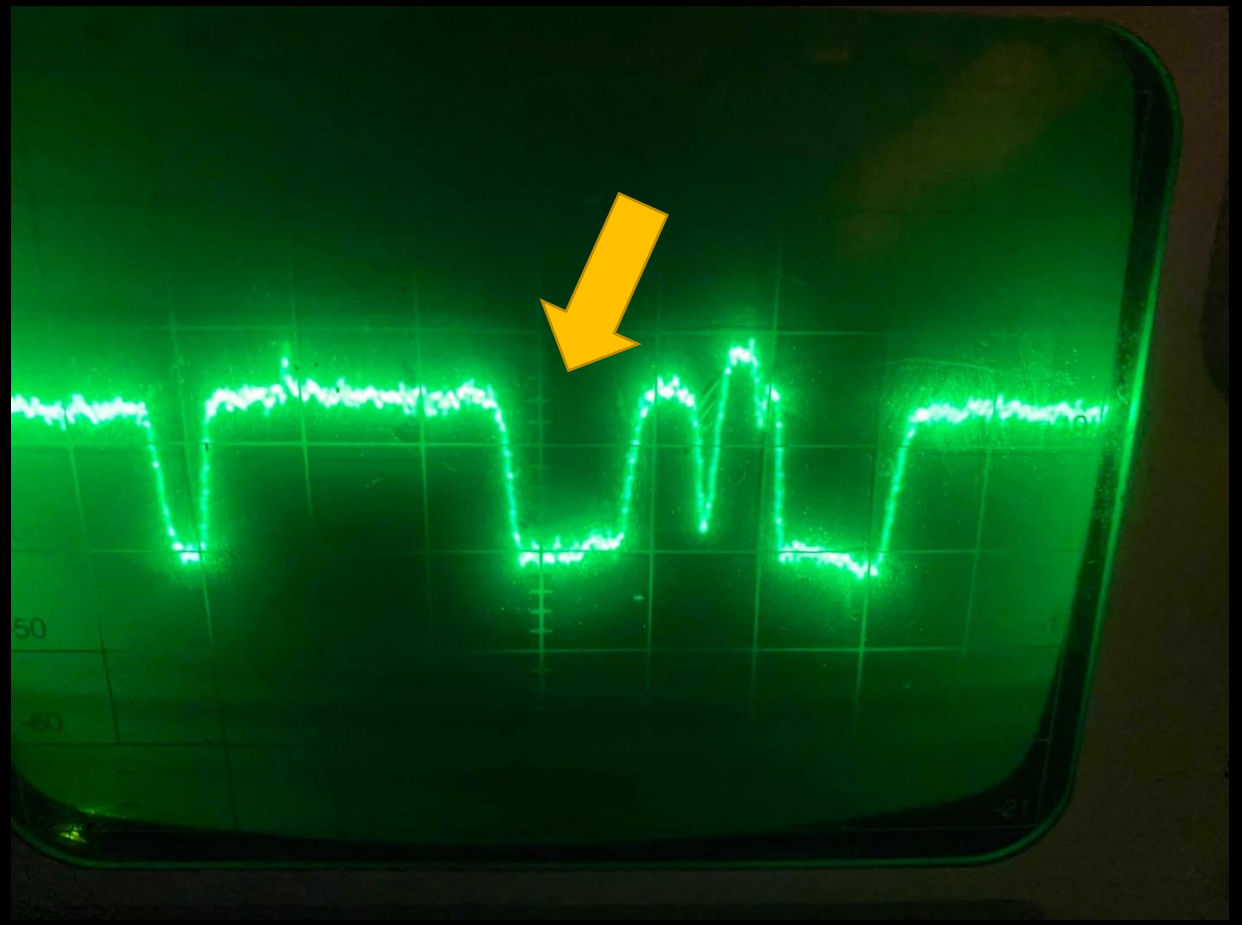
© 2022 Northwestern Telephone and Telegraph
PROPRIETARY AND CONFIDENTIAL

Our Uplink



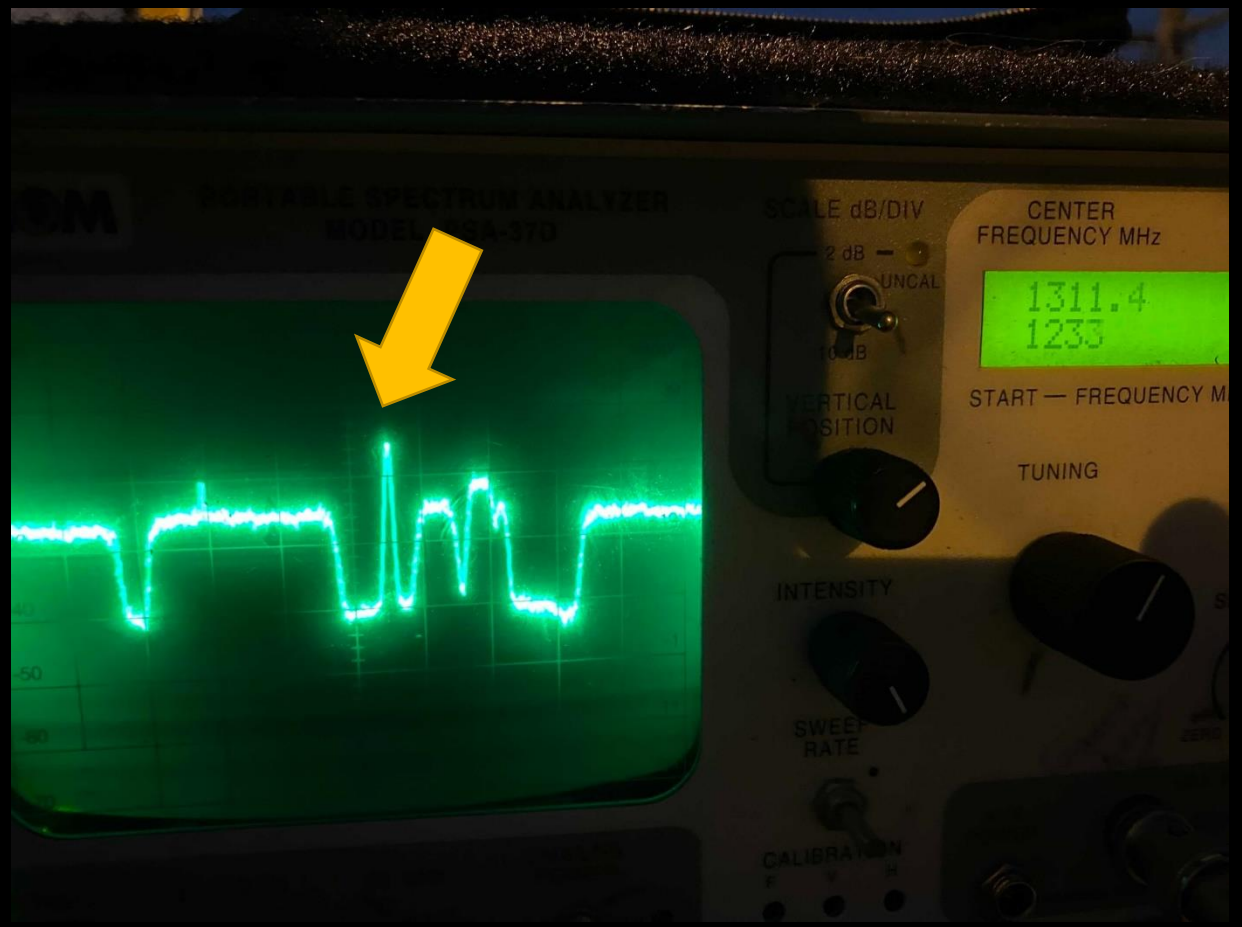
© 2022 Northwestern Telephone and Telegraph
PROPRIETARY AND CONFIDENTIAL

Testing the Uplink



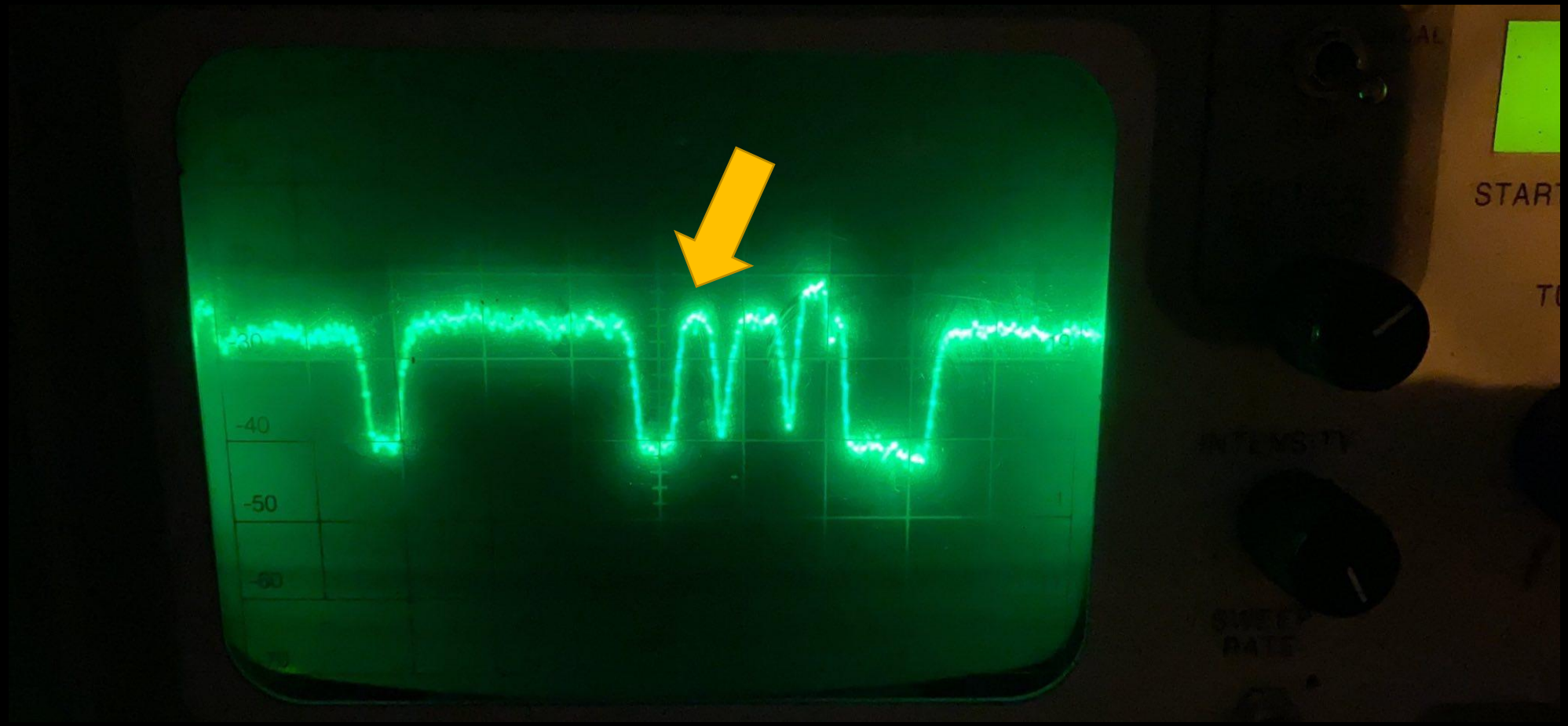
© 2022 Northwestern Telephone and Telegraph
PROPRIETARY AND CONFIDENTIAL

Testing the Uplink



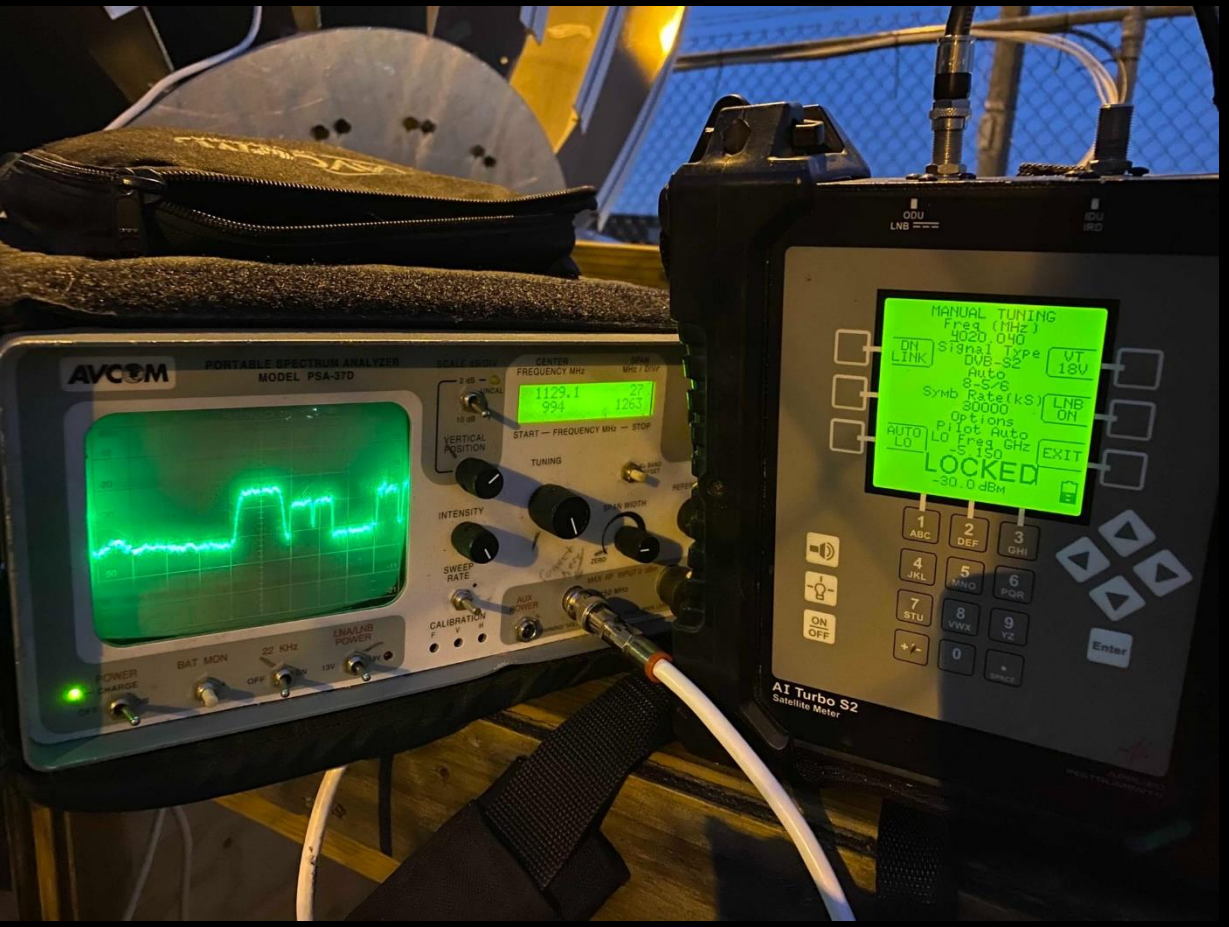
© 2022 Northwestern Telephone and Telegraph
PROPRIETARY AND CONFIDENTIAL

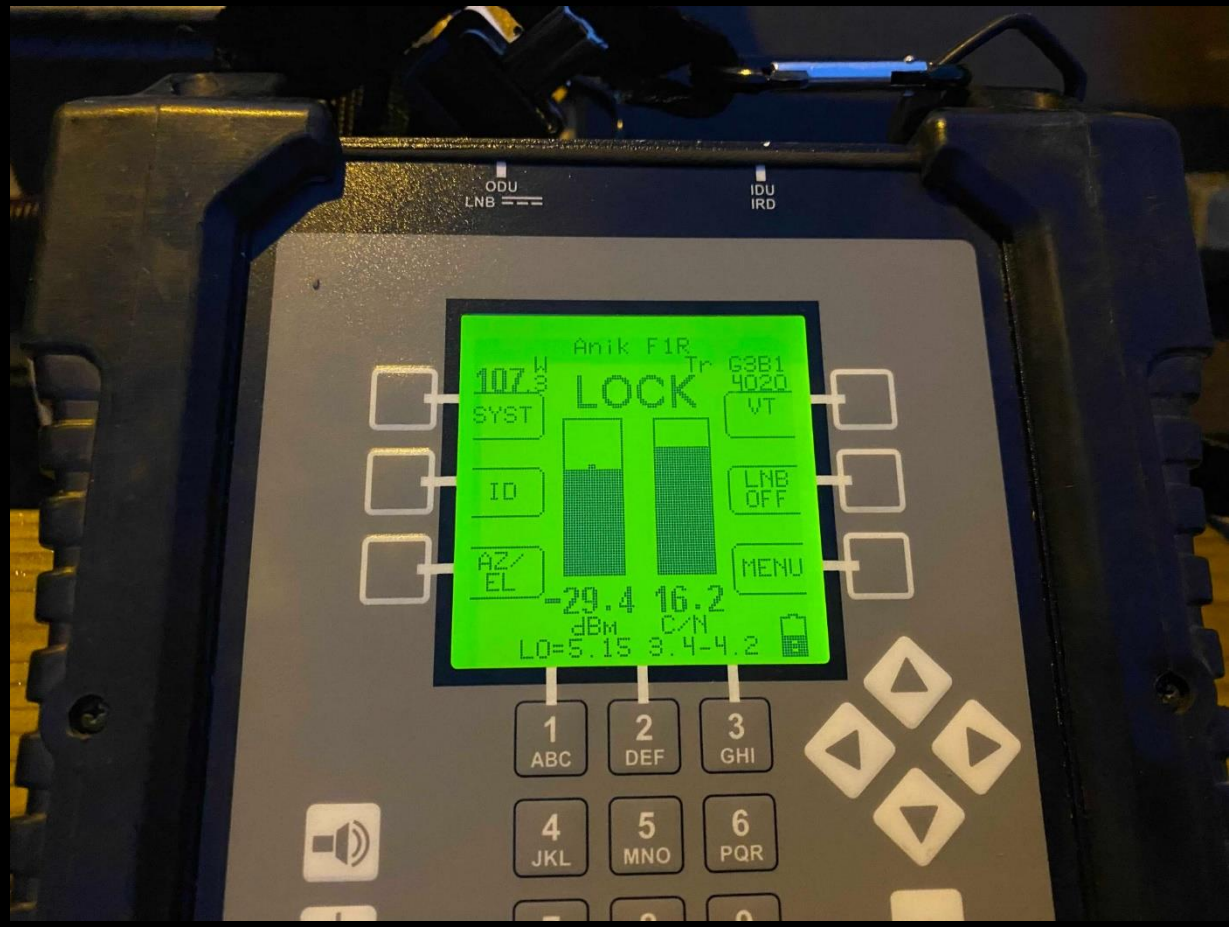
Testing the Uplink



© 2022 Northwestern Telephone and Telegraph
PROPRIETARY AND CONFIDENTIAL

On-Air Testing





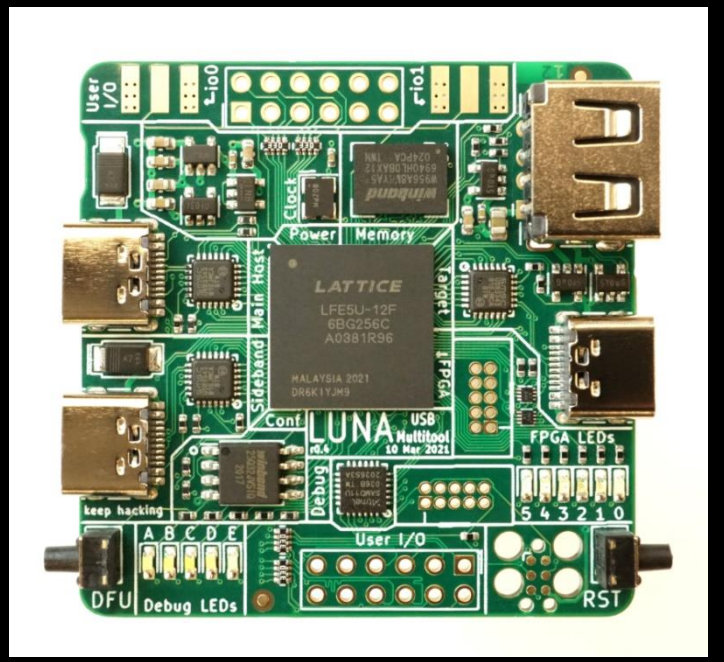
© 2022 Northwestern Telephone and Telegraph
PROPRIETARY AND CONFIDENTIAL

Our Uplink

- **Tandberg Voyager E5740**
  - **Accepts ONLY ASI as input**









© 2022 Northwestern Telephone and Telegraph
PROPRIETARY AND CONFIDENTIAL

Building a DVB-S2 Transmitter

Search or jump to... / Pulls Issues Marketplace Explore

gnuradio / gnuradio Public — Watch 233 — Fork 1.6k — Star 3.7k

Code — Issues 444 — Pull requests 29 — Actions — Projects 5 — Security

main — gnuradio / gr-dtv / examples / — Go to file — Add file

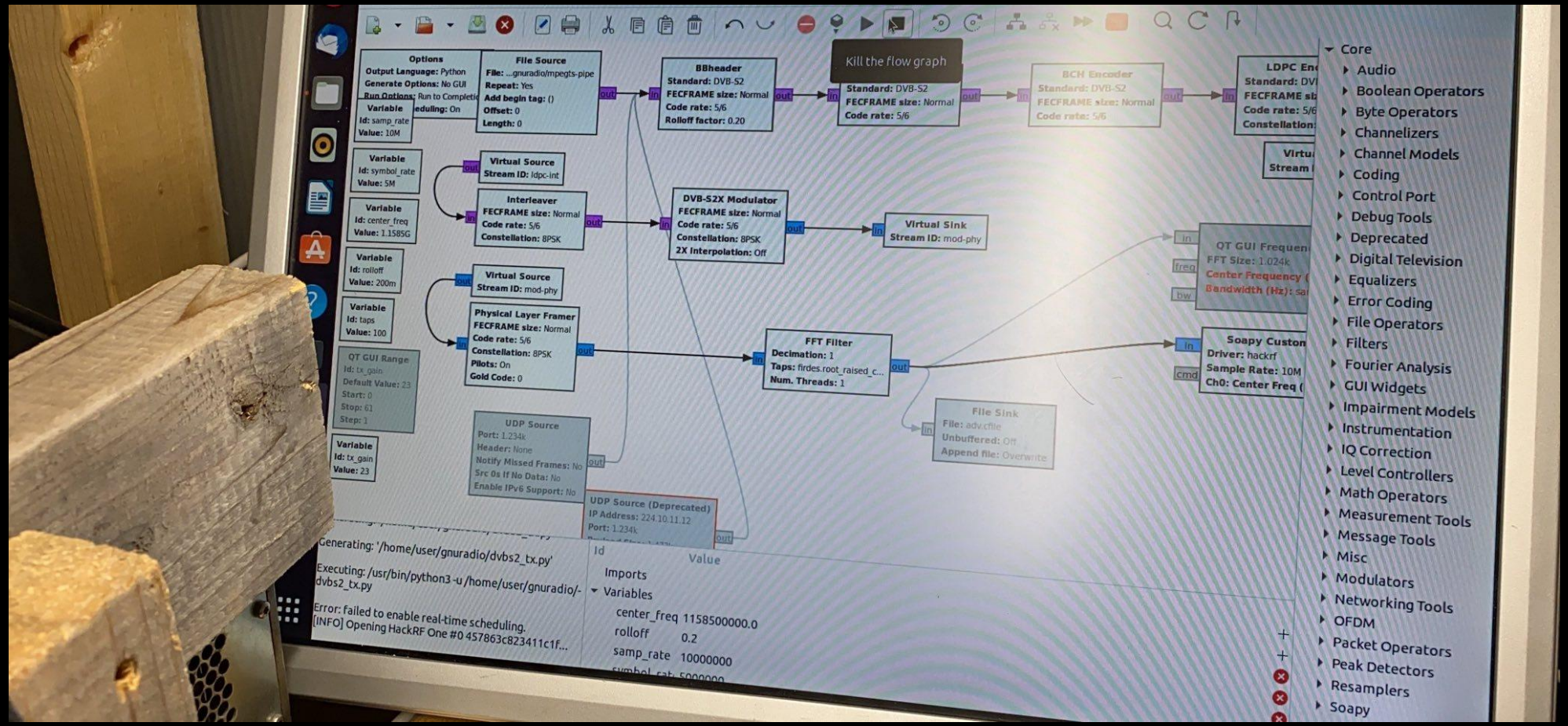
mormj dtv: pep8 formatting ... — on Nov 24, 2021 — History

..		
.gitignore	gitignore: ignore autogen files in example folders	3 years ago
CMakeLists.txt	dtv: enhance ATSC RX example	2 years ago
README.atsc	gr-dtv: Improve ATSC transmitter performance with Rotator block.	6 years ago
README.catv	dtv: Add 256QAM mode to ITU-T J.83B transmitter.	5 years ago
README.dvbs	gr-dtv: Update example flow graphs to Qt.	6 years ago
README.dvbs2	gr-dtv: Add DVB-S2 transmitter.	7 years ago
README.dvbt	Add DVB-T receiver flow graph.	7 years ago
README.dvbt2	dtv: Add conditional compile for DVB-T2 PAPR reduction validation.	5 years ago
atsc_ctrlport_monitor.py	dtv: pep8 formatting	4 months ago
catv_tx_256qam.grc	examples: Repair all examples affected by commit 91e9ddf.	6 months ago
catv_tx_64qam.grc	examples: Repair all examples affected by commit 91e9ddf.	6 months ago
dvbs2_tx.grc	examples: Repair all examples affected by commit 91e9ddf.	6 months ago



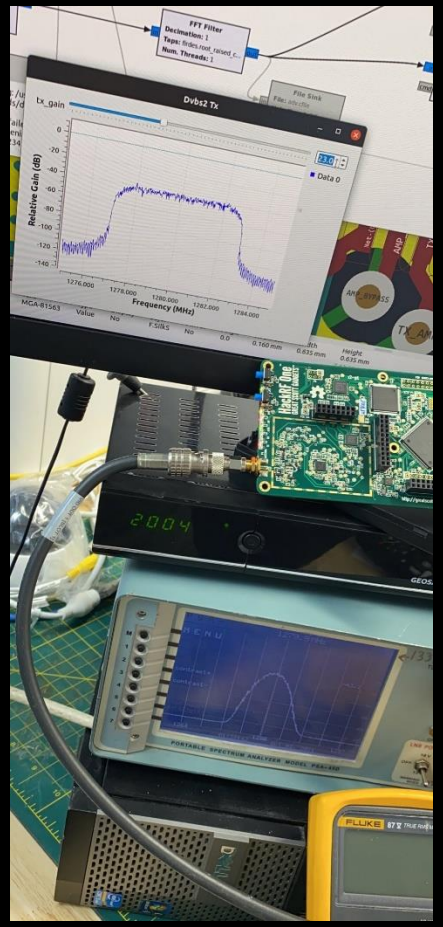
© 2022 Northwestern Telephone and Telegraph
PROPRIETARY AND CONFIDENTIAL

Building a DVB-S2 Transmitter

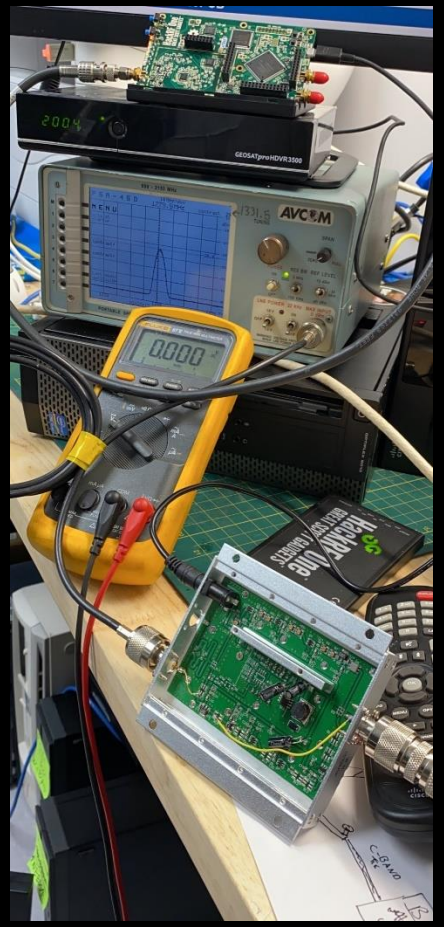


© 2022 Northwestern Telephone and Telegraph
PROPRIETARY AND CONFIDENTIAL

Building a DVB-S2 Transmitter







© 2022 Northwestern Telephone and Telegraph
PROPRIETARY AND CONFIDENTIAL

Building a DVB-S2 Transmitter



© 2022 Northwestern Telephone and Telegraph
PROPRIETARY AND CONFIDENTIAL

Test stream: http://www.w6rz.net/sweetnothing8psk_184_56.ts

MPEG 2 Transport Streams

- **Carries one or more programs/channels over a continuous stream**
- **Used extensively: OTA TV, Cable TV, Satellites, even DOCSIS!**
- **Multiplexes media (ES) streams together, each assign its own PID**
- **Channel maps associate multiple ESes into a single program**
  - **e.g., one video stream, two audio streams in different languages**
  - **Can theoretically do multiple video streams, which some DVDs used**
  - **Codec-agnostic: can do H.262/H2.64/H.265/AC-3/MP3/AAC/etc.**

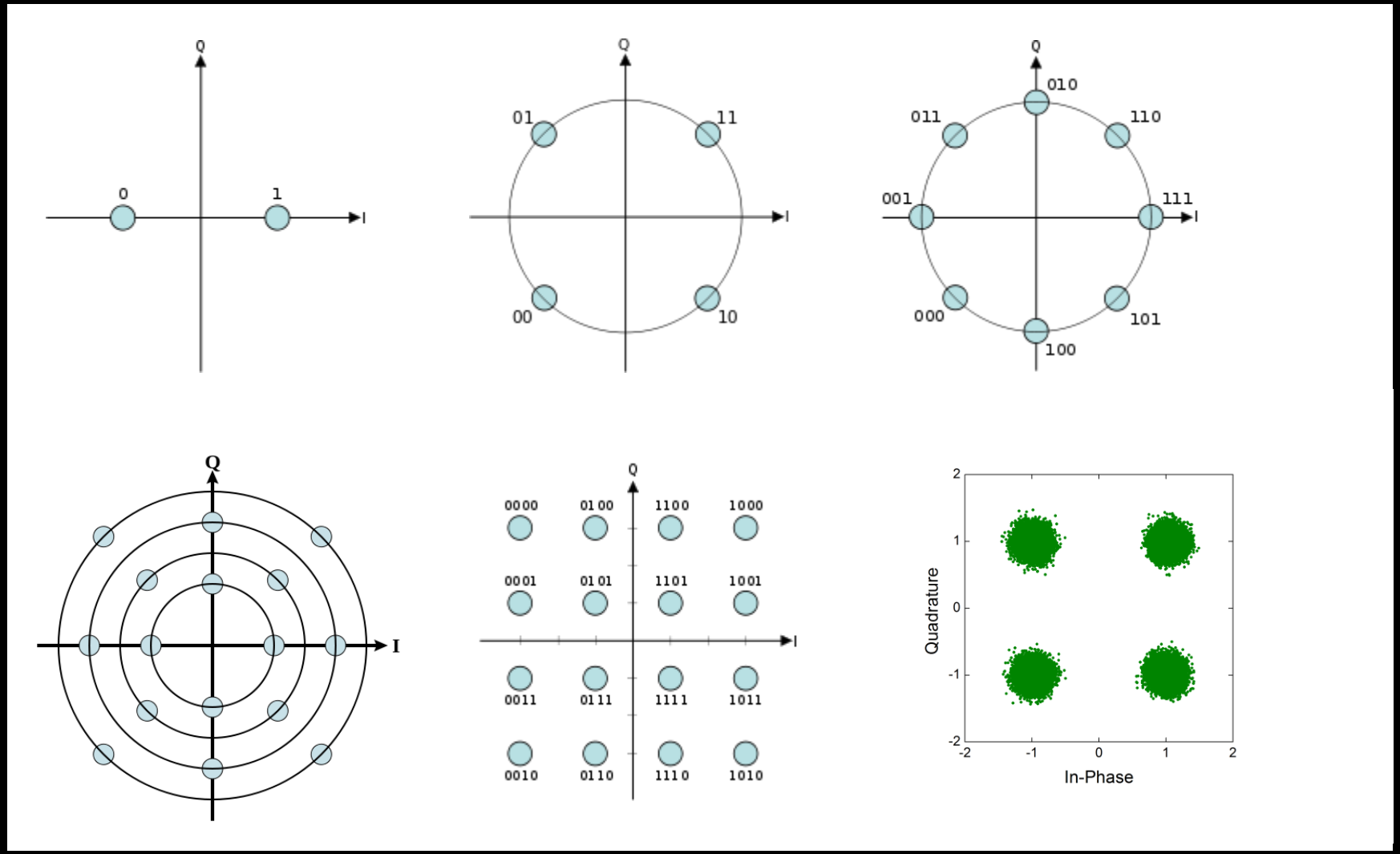
© 2022 Northwestern Telephone and Telegraph
PROPRIETARY AND CONFIDENTIAL

MPEG 2 Transport Streams

- **Broadcast M2TS requires extremely specific bit rates**
- **Derived from modulation parameters, e.g.,**
  - **Mode: (8VSB vs. PSK vs. OFDM)**
  - **Occupied bandwidth (e.g., 5-8 MHz)**
  - **Constellation / number of bits per symbol**
  - **Symbols per second**
  - **Error correction overhead (e.g., 1/2, 2/3, 3/4, 5/6, 7/8)**
    - **Simple form: represent data as a degree (n-1) polynomial**
    - **Advanced forms can take advantage of “soft-decoding” (e.g., closeness to valid point)**
- **Null packets (PID 0x1FFF) are inserted to keep bitrate constant**

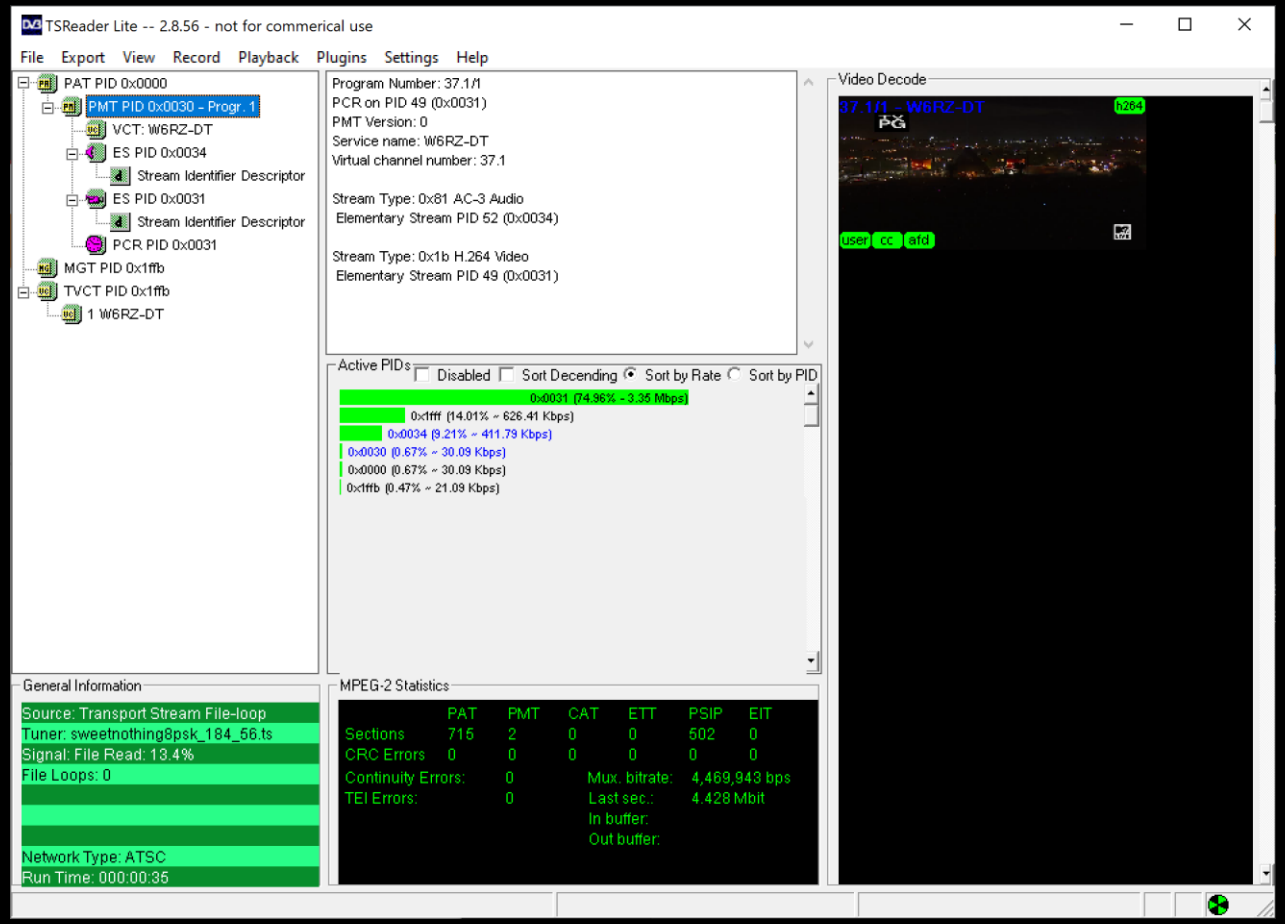
© 2022 Northwestern Telephone and Telegraph
PROPRIETARY AND CONFIDENTIAL

Constellation Diagrams



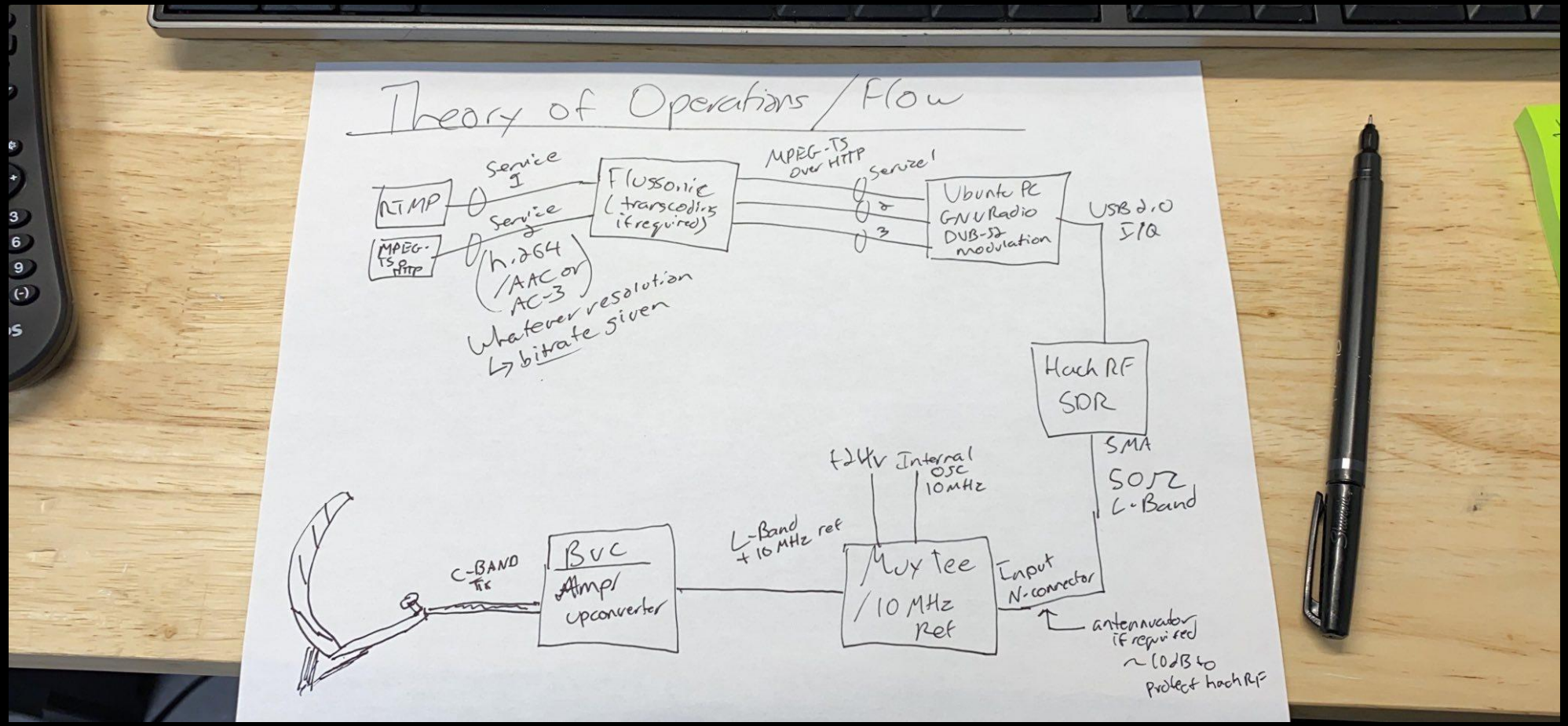
Images by Splash (Wikipedia)

MPEG 2 Transport Streams



© 2022 Northwestern Telephone and Telegraph
PROPRIETARY AND CONFIDENTIAL

The Complete Broadcast Chain



© 2022 Northwestern Telephone and Telegraph
PROPRIETARY AND CONFIDENTIAL

Media Chain

- **OBS generates RTMP source, pointed at our server (nginx)**
- **Flussonic ingests RTMP, performs PID remapping to support multiple programs, and produces M2TS over HTTP**
- **tsduck muxes multiple M2TSes together at final bitrate**
  - **Inserts null packets as needed**
- **Resulting stream sent to GNU Radio applet over socket**

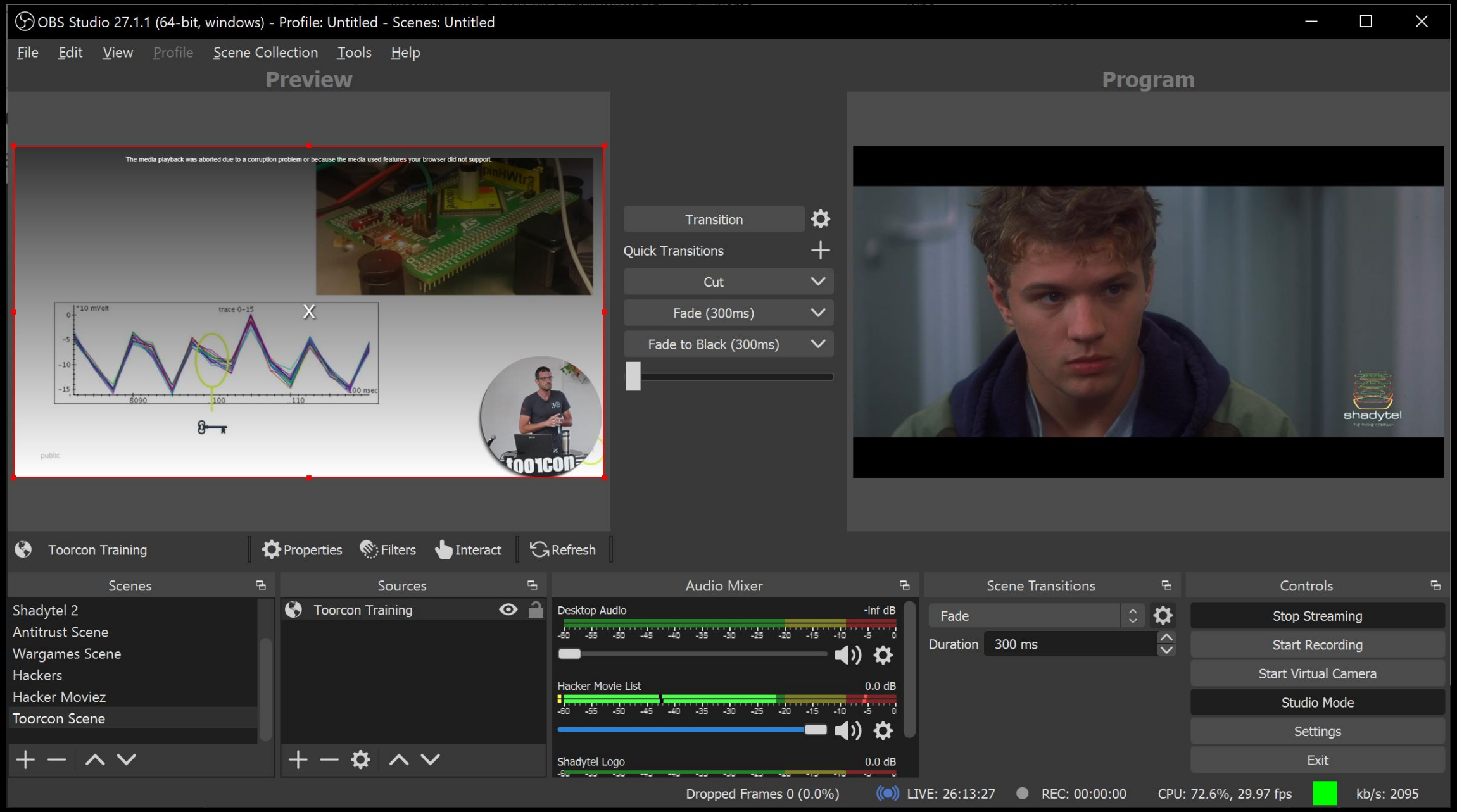
© 2022 Northwestern Telephone and Telegraph
PROPRIETARY AND CONFIDENTIAL

Content Selection

- **What do we put in a hacker satellite broadcast?**
- **Why not an entire con?**
- **Satellite was going away in November 2021**
- **Got permission to restream Toorcon San Diego**
  - **Normally $50!**

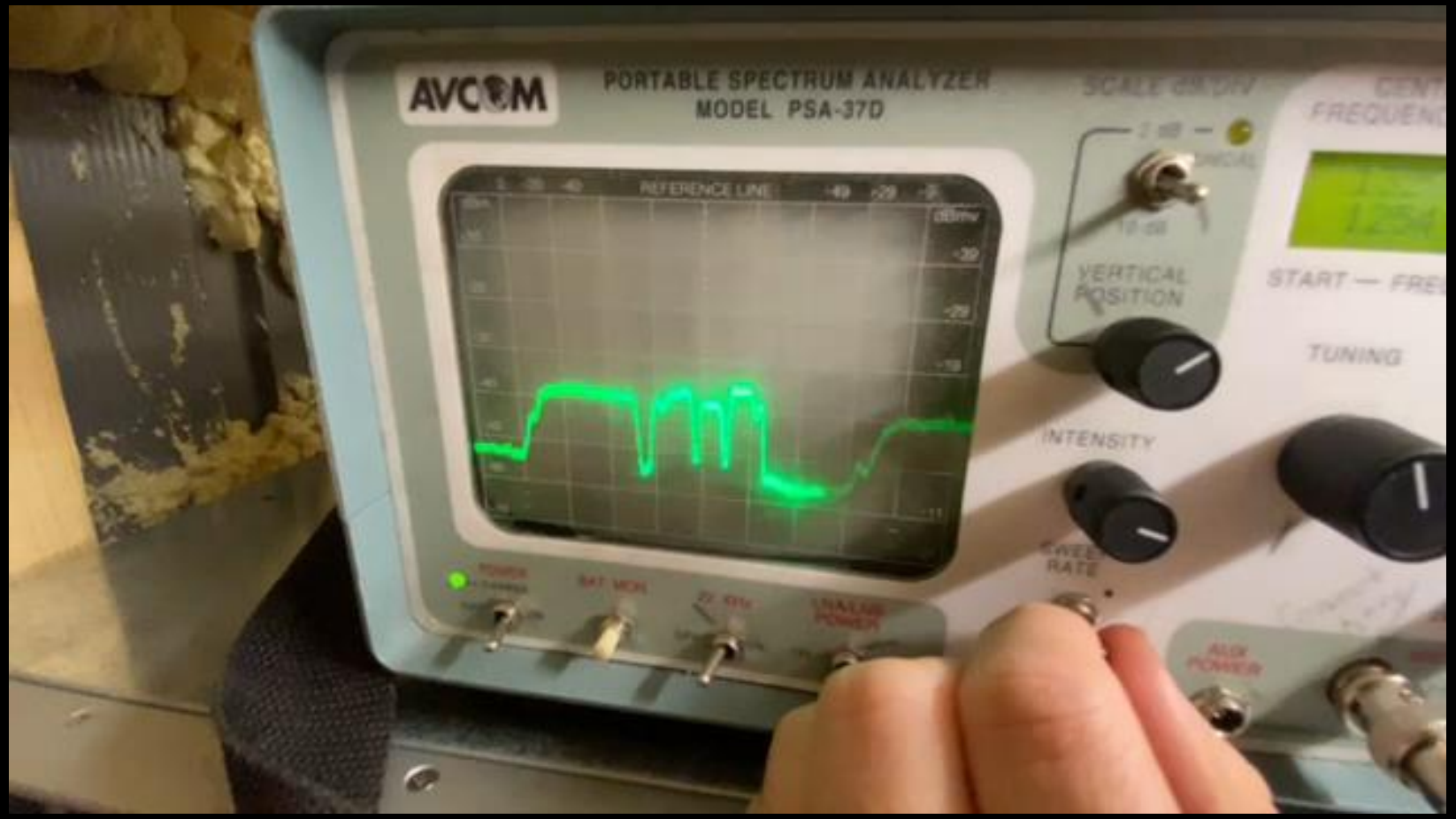


© 2022 Northwestern Telephone and Telegraph
PROPRIETARY AND CONFIDENTIAL



© 2022 Northwestern Telephone and Telegraph
PROPRIETARY AND CONFIDENTIAL

On-Air Testing



© 2022 Northwestern Telephone and Telegraph
PROPRIETARY AND CONFIDENTIAL

On-Air Testing



© 2022 Northwestern Telephone and Telegraph
PROPRIETARY AND CONFIDENTIAL

Receiving ShadyVision



© 2022 Northwestern Telephone and Telegraph
PROPRIETARY AND CONFIDENTIAL

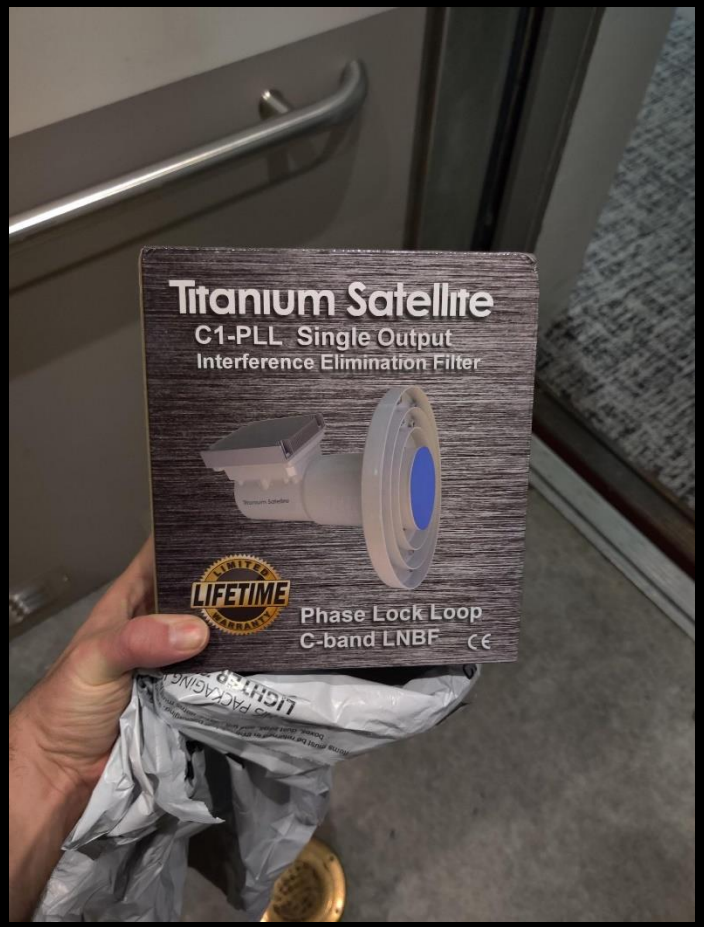
Receiving ShadyVision

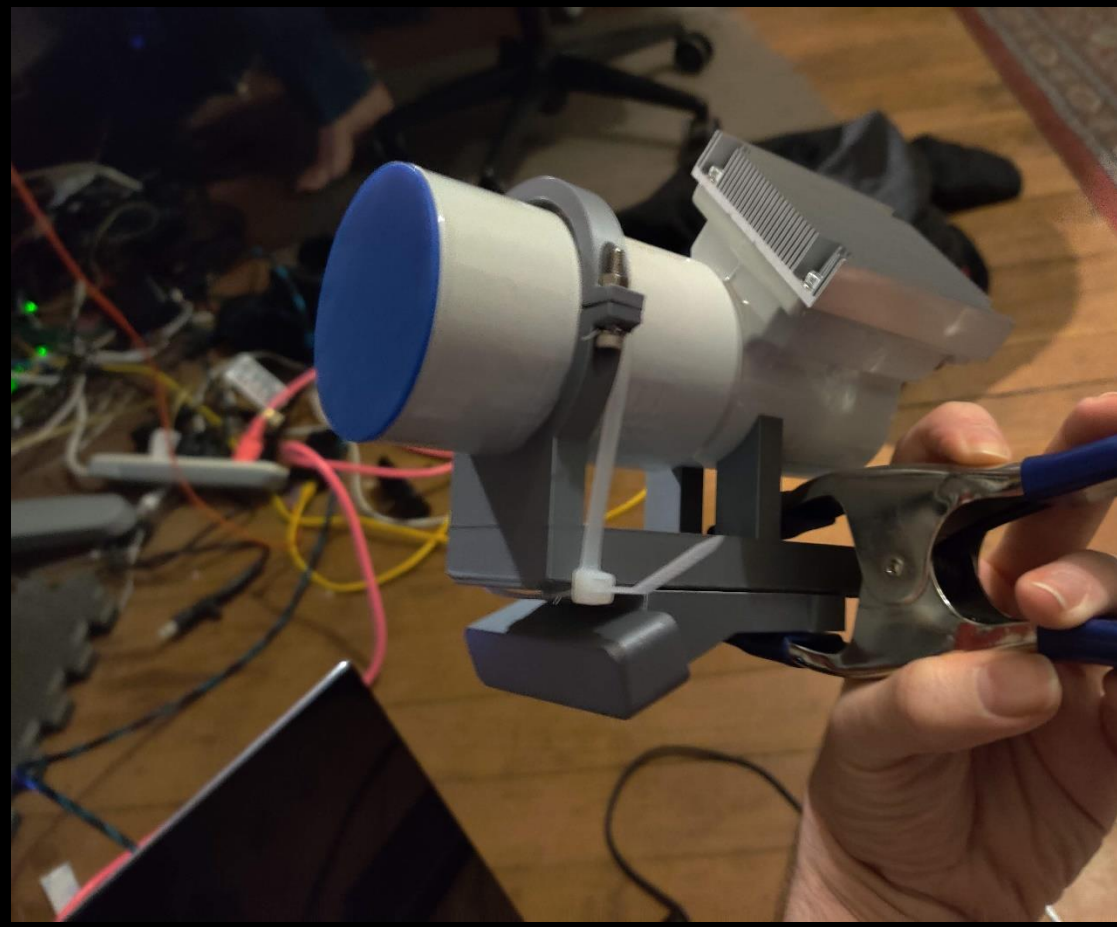
- **CAUTION: Speculation below!**
- **About ~16 C/N at transmitter site (should be better in CONUS)**
- **Reusing a DirecTV dish would lose us about 14 dB**
- **… but remember, we control the modulation parameters!**
  - **DVB-S2, QPSK, 3/5 FEC requires 2.2 C/N**
  - **DVB-S2, QPSK, 1/2 FEC requires 1.0 C/N**
  - **DVB-S2, QPSK, 1/4 FEC requires -2.4 C/N**
    - **At 5000 kSym/s w/ pilot, effective throughput is 2388 kbps w/ ~4 dB link margin**
    - **DEF CON documentary at 1080p h265 *averages* 1595 kbps**

© 2022 Northwestern Telephone and Telegraph
PROPRIETARY AND CONFIDENTIAL

Receiving ShadyVision



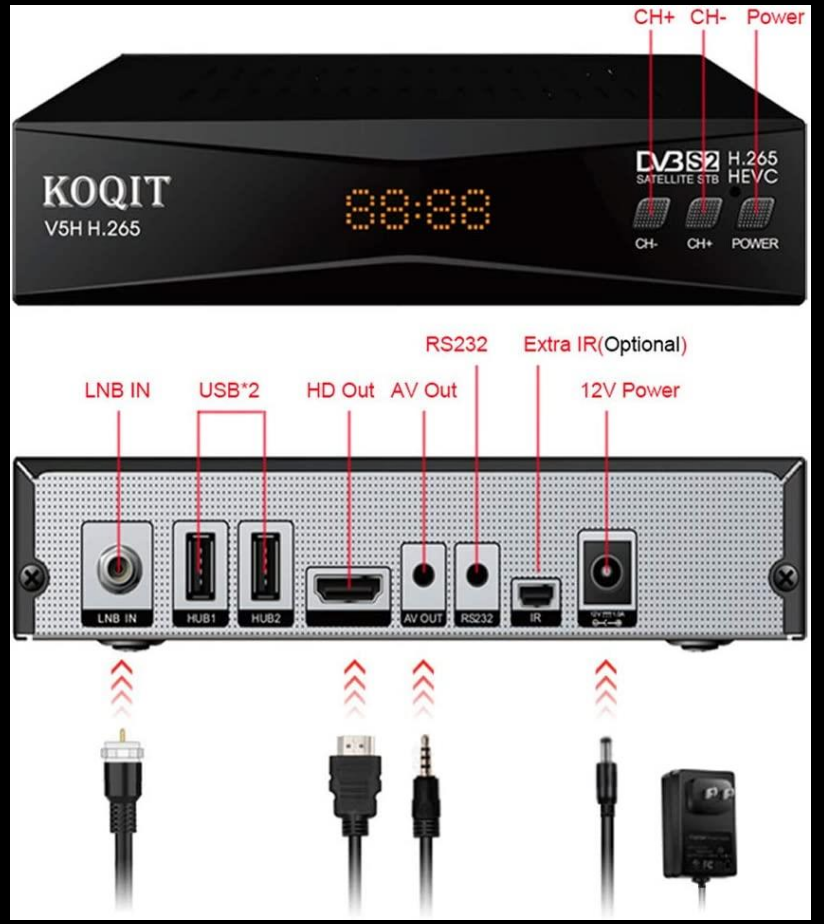




© 2022 Northwestern Telephone and Telegraph
PROPRIETARY AND CONFIDENTIAL

Receiving ShadyVision





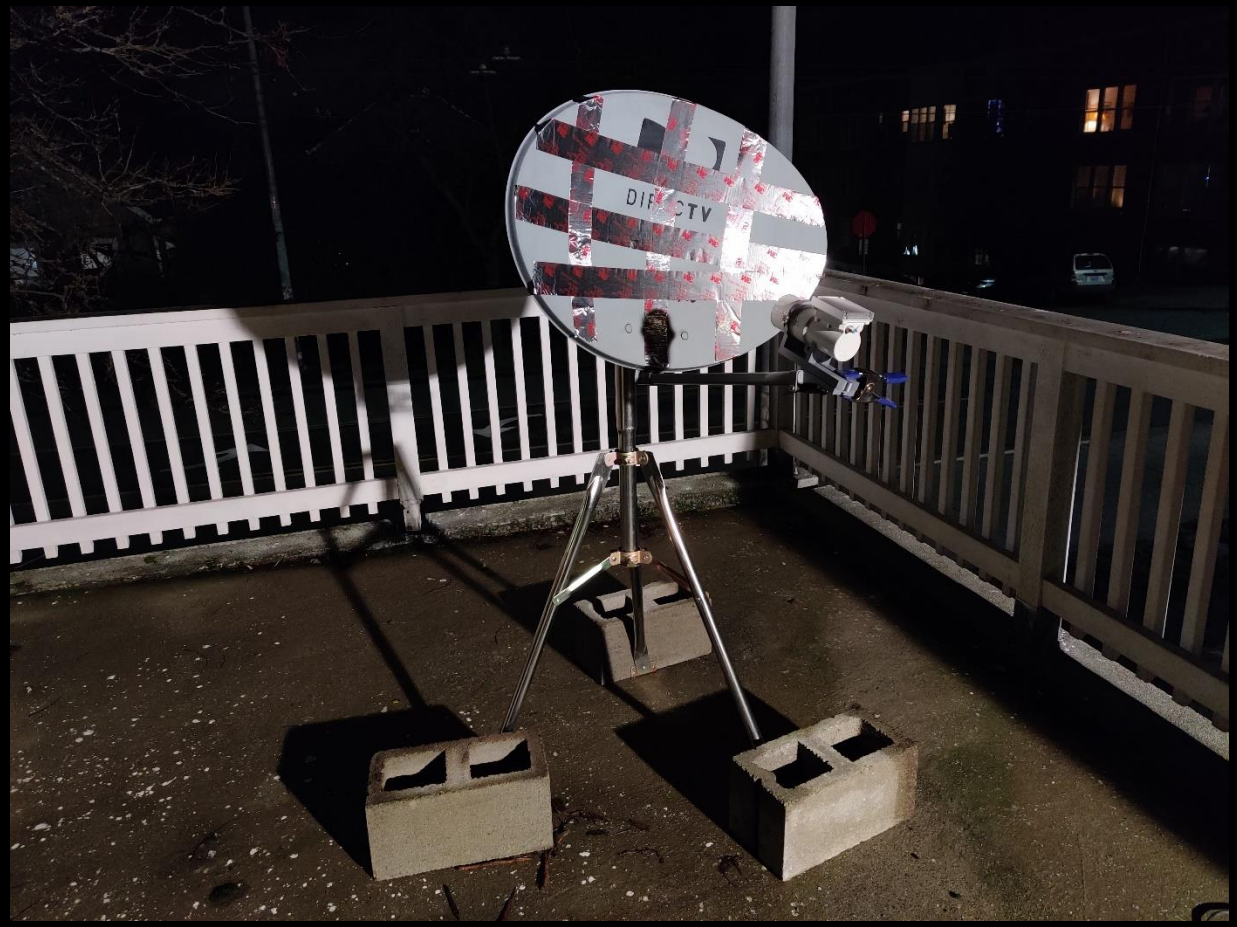
© 2022 Northwestern Telephone and Telegraph
PROPRIETARY AND CONFIDENTIAL

Receiving ShadyVision



© 2022 Northwestern Telephone and Telegraph
PROPRIETARY AND CONFIDENTIAL

Receiving ShadyVision





© 2022 Northwestern Telephone and Telegraph
PROPRIETARY AND CONFIDENTIAL

Receiving ShadyVision



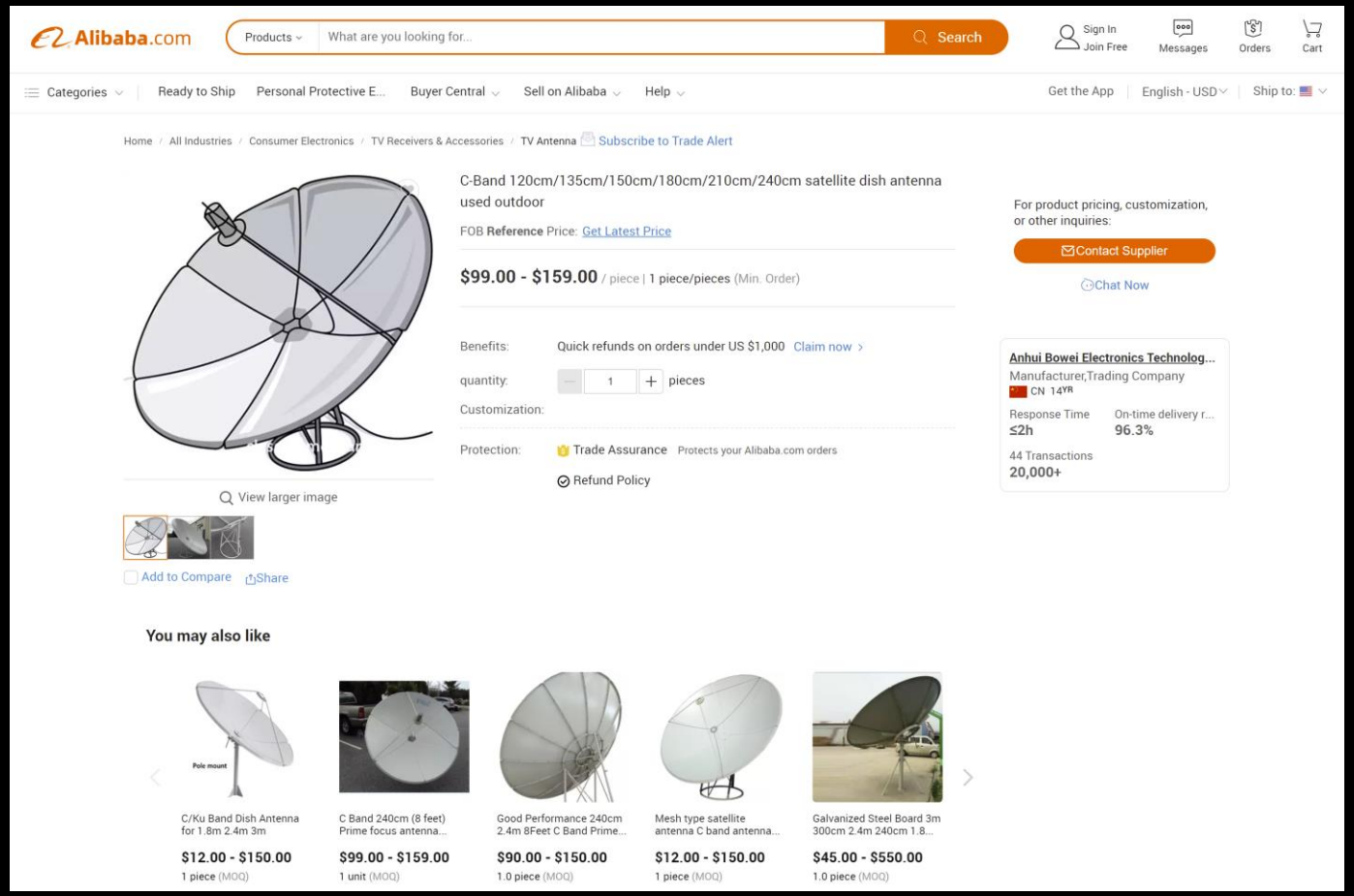
© 2022 Northwestern Telephone and Telegraph
PROPRIETARY AND CONFIDENTIAL

Receiving ShadyVision



© 2022 Northwestern Telephone and Telegraph
PROPRIETARY AND CONFIDENTIAL

Receiving ShadyVision



© 2022 Northwestern Telephone and Telegraph
PROPRIETARY AND CONFIDENTIAL

Setting Up Your Own Broadcasts

- **For C band satellite broadcasts, you need:**
  - **A LARGE dish**
  - **A way to upconvert to ~6 GHz**
  - **A surprisingly small amplifier (we operated at ~15 Watts)**
  - **Permission ☺**

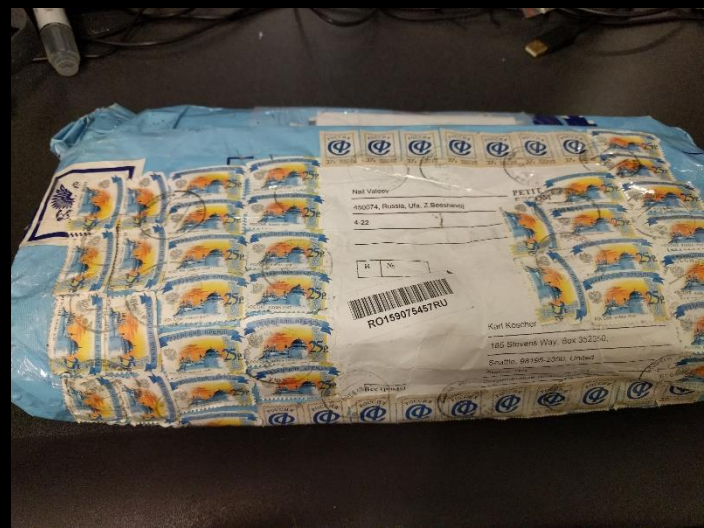
- **Ku band operation requires more power and components that can run up to ~14.5 GHz**
  - **Smaller wavelength means smaller dishes**
  - **Probably way more supply on eBay**

© 2022 Northwestern Telephone and Telegraph
PROPRIETARY AND CONFIDENTIAL

Setting Up Your Own Broadcasts

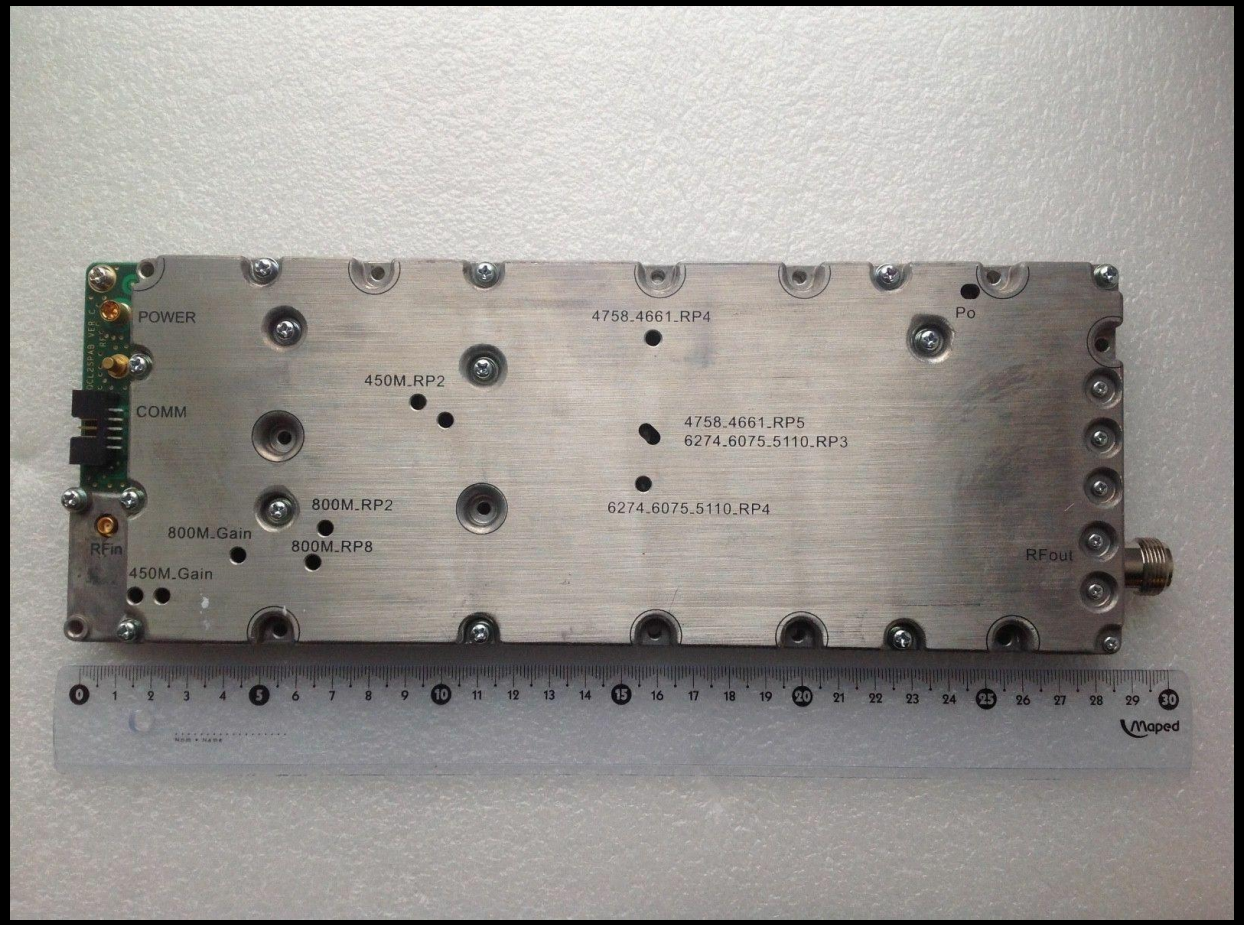
- **Almost nothing in this talk is specific to satellites!**

- **Use DVB-T for terrestrial broadcasts**
  - **Everyone has a tuner – the RTL-SDR**
  - **Tweak modulation parameters (symbol rate, constellation, FEC) as desired to meet your link budget**
  - **Need to replace amplifier/antenna**
    - **Existing Amateur TV amplifiers? (Needs to be linear)**
    - **Sketchy Russian LTE amps??**
      - **Overlaps UHF band and 70cm Amateur spectrum**
    - **Please filter and monitor your emissions!**



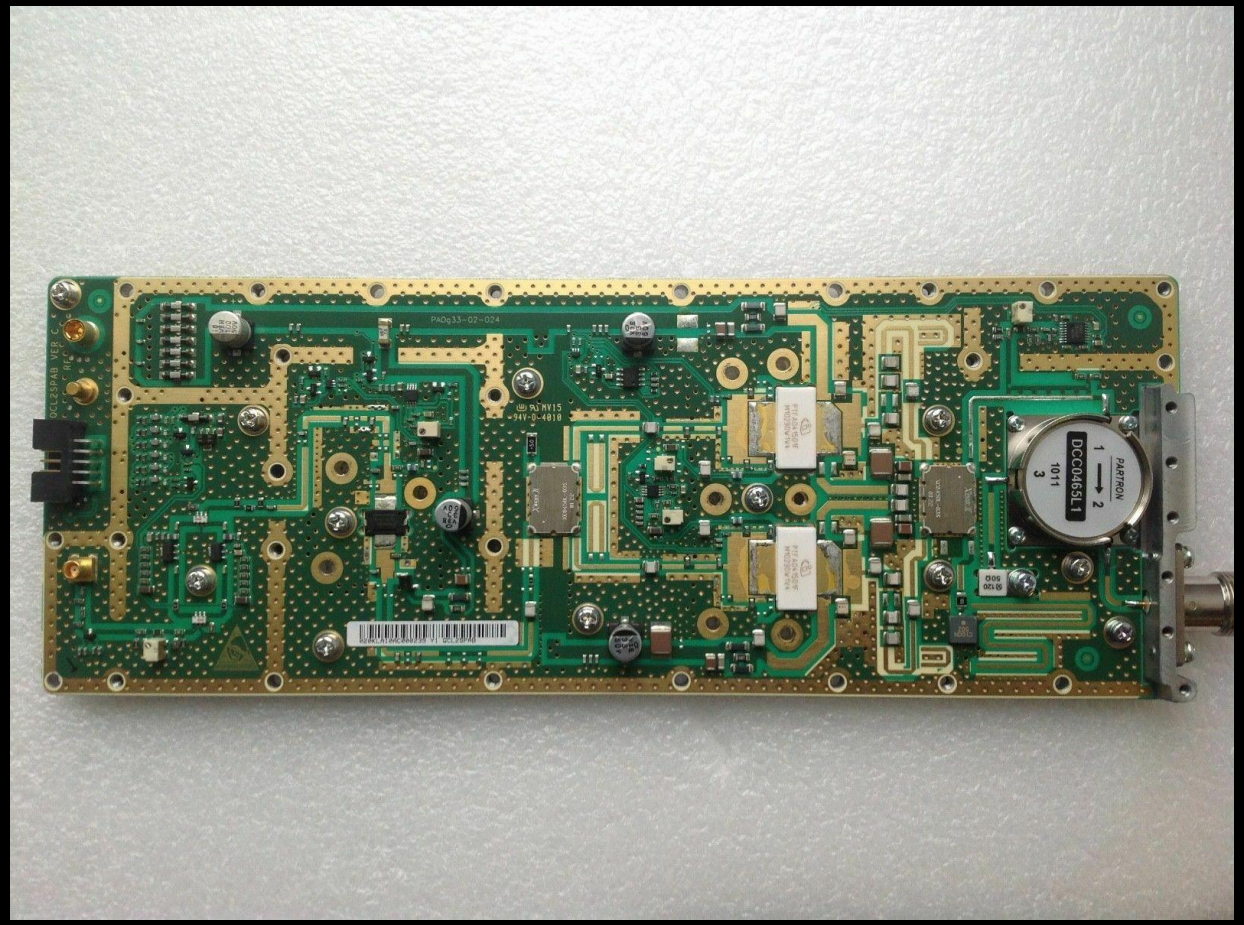
© 2022 Northwestern Telephone and Telegraph
PROPRIETARY AND CONFIDENTIAL

Setting Up Your Own Broadcasts



© 2022 Northwestern Telephone and Telegraph
PROPRIETARY AND CONFIDENTIAL

Setting Up Your Own Broadcasts



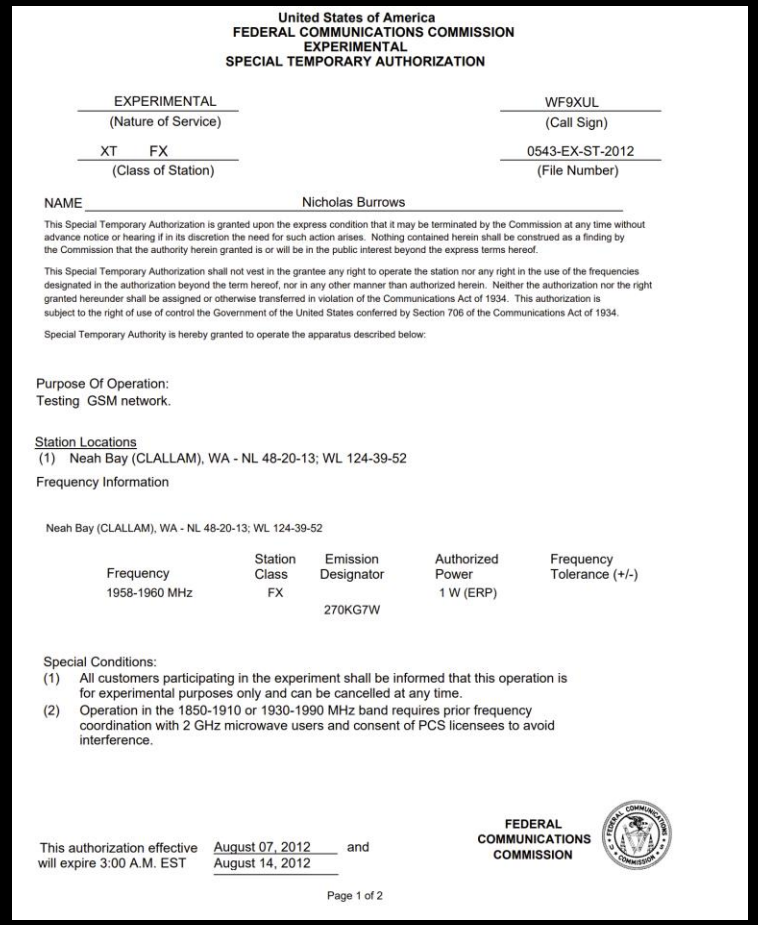
© 2022 Northwestern Telephone and Telegraph
PROPRIETARY AND CONFIDENTIAL

Setting Up Your Own Broadcasts

- **… and of course, permission ☺**
- **One approach: constrain transmissions to "information bulletins" "directed only to amateur operators consisting solely of subject matter of direct interest to the amateur service." (i.e., this talk)**
- **Or: Obtain a Special Temporary Authority (STA) from the FCC for testing in un-usued TV whitespace**
  - **Used by Shadytel to run a GSM network at Toorcamp one year**

© 2022 Northwestern Telephone and Telegraph
PROPRIETARY AND CONFIDENTIAL

Setting Up Your Own Broadcasts



United States of America
FEDERAL COMMUNICATIONS COMMISSION
EXPERIMENTAL
SPECIAL TEMPORARY AUTHORIZATION

EXPERIMENTAL	WF9XUL
(Nature of Service)	(Call Sign)
XT FX	0543-EX-ST-2012
(Class of Station)	(File Number)

NAME Nicholas Burrows

This Special Temporary Authorization is granted upon the express condition that it may be terminated by the Commission at any time without advance notice or hearing if in its discretion the need for such action arises. Nothing contained herein shall be construed as a finding by the Commission that the authority herein granted is or will be in the public interest beyond the express terms hereof.

This Special Temporary Authorization shall not vest in the grantee any right to operate the station nor any right in the use of the frequencies designated in the authorization beyond the term hereof, nor in any other manner than authorized herein. Neither the authorization nor the right granted hereunder shall be assigned or otherwise transferred in violation of the Communications Act of 1934. This authorization is subject to the right of use of control the Government of the United States conferred by Section 706 of the Communications Act of 1934.

Special Temporary Authority is hereby granted to operate the apparatus described below:

Purpose Of Operation:
Testing GSM network.

Station Locations
(1) Neah Bay (CLALLAM), WA - NL 48-20-13; WL 124-39-52

Frequency Information

Neah Bay (CLALLAM), WA - NL 48-20-13; WL 124-39-52

Frequency	Station Class	Emission Designator	Authorized Power	Frequency Tolerance (+/-)
1958-1960 MHz	FX	270KG7W	1 W (ERP)	

Special Conditions:
(1) All customers participating in the experiment shall be informed that this operation is for experimental purposes only and can be cancelled at any time.
(2) Operation in the 1850-1910 or 1930-1990 MHz band requires prior frequency coordination with 2 GHz microwave users and consent of PCS licensees to avoid interference.

This authorization effective August 07, 2012 and will expire 3:00 A.M. EST August 14, 2012

FEDERAL COMMUNICATIONS COMMISSION

Page 1 of 2

The purpose of the test will be to verify functionality of an Open Source GSM network design in an outdoor test range under load of up to 1,000 test users. For one week, users will send and receive text messages and place voice-calls to various services and other users while the system is under observation. System will consist of several Base Stations to provide experimental service to test users. Test users will be notified that the system is experimental, and access will be limited to SIM cards provided to test users. Test will occur for the duration and in the location of the Toorcamp Conference (08/06/2012-08/12/2012). The conference provides an ideal source of informed test users for this test.

Equipment is Commercial PicoCells (FCC ID: PEI-INSITE-1900), with the Test Users using standard quad-band GSM consumer devices. The PicoCells will be located below the surrounding tree-line and structures in the test site to help stress the system in a poor RF environment and limiting the system to line-of-sight operation.

© 2022 Northwestern Telephone and Telegraph
PROPRIETARY AND CONFIDENTIAL

What Is This Good For?!

- **With a large enough audience, *very* efficient use of bandwidth**
  - **e.g., hacker events with limited WiFi**
  - **Range can be significantly larger**

- **Works even if all network links are down**

- **A way to get information across borders?**
  - **Works both ways: the EU can’t block direct reception of RT**
  - **Caveat: the dishes are large and might also be restricted**

© 2022 Northwestern Telephone and Telegraph
PROPRIETARY AND CONFIDENTIAL



© 2022 Northwestern Telephone and Telegraph
PROPRIETARY AND CONFIDENTIAL



© 2022 Northwestern Telephone and Telegraph
PROPRIETARY AND CONFIDENTIAL