HACK THE ... HEMISPHERE!!!

shadytel
THE PHONE COMPANY

Karl Koscher (@supersat)
Andrew Green
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

Joined June 2010

Shadytel @shadytel · 28 Jun 2015

#pride2015 #billingexcellence #twistedpride

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!
ShadyTel Phone Directory
As of July 31 at 1am

3002 CUSJON
3101 STAFF
3099 Tree Shady Camp
3333 the LD
3210 Duncan’s Hatch
3102 Staff Camp
3216 RV Franklin Hu
3999 Annc cct
3133 T Prophet
3996 Cabins DSL Drop
3825 Nick F
3826 Milliways
3003 Black Lodge 1
3004 Black Lodge 2
3005 Garett (ala’s)
3232 Alex’s
3323 Alex
3007 PDX
3008 Noisebridge 1
3009 Noisebridge 2
3012 Hals
3011 Leviathan
3217 RF pail
3323 Alex
3021 Cabin 9
3022 Hack Casual
3023 Registration
3667 Door Phone
3013 Ninjafel 1
3014 Ninjafel 2
3024 Demoprint
3015 Anything
3016 Nick Lewis (Nerd Creation Lab)
3411 TC Info Desk
3337 Caesar
3020 Nen9
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
Shadytel @shadytel · Oct 1, 2021

LEO isn't cool.

You know what's cool?

GEO.
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
An Unprecedented Opportunity...
Anik F1R
Strong North American coverage in C- and Ku-band frequencies

Key Facts

- 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

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
Anik F1R Transponder Configuration

Uplink

Downlink

North America

© 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
Testing the Uplink
Testing the Uplink
Testing the Uplink
Our Uplink

- Tandberg Voyager E5740
  - Accepts ONLY ASI as input
Building a DVB-S2 Transmitter
Building a DVB-S2 Transmitter
Building a DVB-S2 Transmitter
Building a DVB-S2 Transmitter

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.
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
MPEG 2 Transport Streams
The Complete Broadcast Chain
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
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!
On-Air Testing
On-Air Testing
Receiving ShadyVision

SOON

© 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
Receiving ShadyVision
Receiving ShadyVision
Receiving ShadyVision
Receiving ShadyVision
Receiving ShadyVision
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!
Setting Up Your Own Broadcasts
Setting Up Your Own Broadcasts
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-used TV whitespace
  • Used by Shadytel to run a GSM network at Toorcamp one year
Setting Up Your Own Broadcasts

United States of America
FEDERAL COMMUNICATIONS COMMISSION
EXPERIMENTAL
SPECIAL TEMPORARY AUTHORIZATION

NAME: Nicholas Burrell

EXPERIMENTAL (Nature of Service)
W6FNL (Call Sign)
XT (Date of Station)
FX (File Number)
0543-EK-ST-2012

Frequency Information

Station Class Frequency authorized
F2 1795-1995 MHz

Equipment Information

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.
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