Current Board of Directors

Charlie NN3V President
Joe K6JPE Vice President
Jim NE6O Director
Gregg KI6RXX Director
Gary W6GDK Secretary
Richard KJ6WUY Treasurer
Dennis Baca KD6TUJ Repeater Site Chair
Glen KJ6ZQH Membership
Mark KF6WTN Repeater Technical Chair

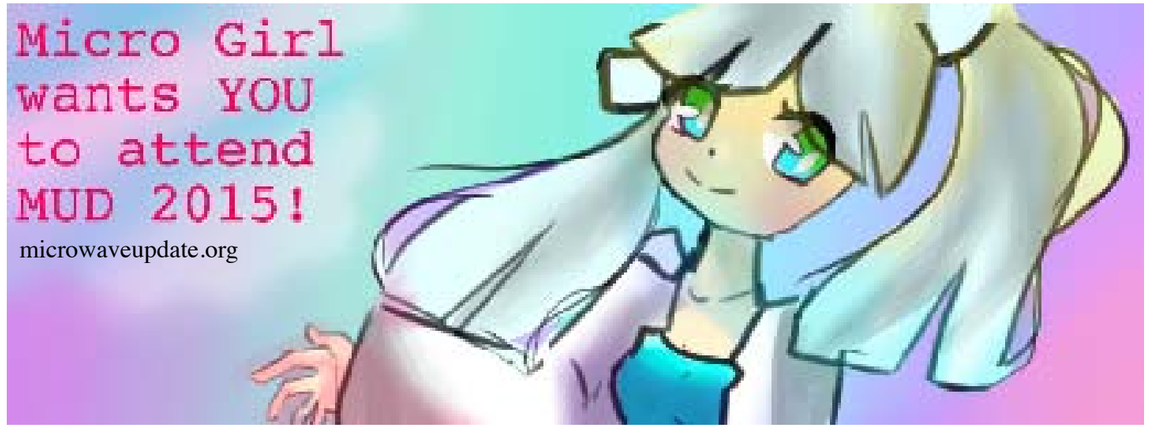
Elections for 2016 Board will be held at the November 2015 membership meeting.

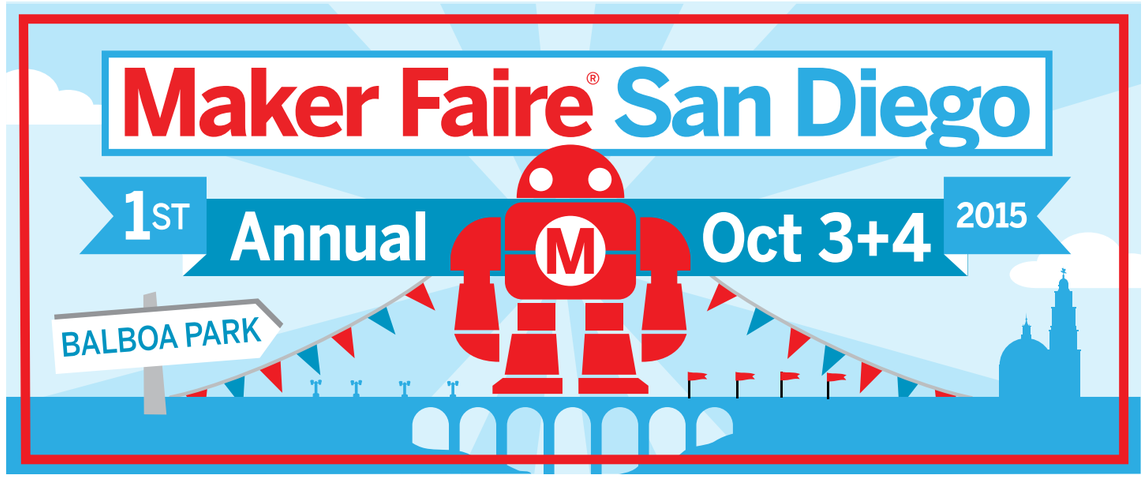
Save the Date

Club Meeting	Board Meeting	Club Events
7 October 2015	**14 October 2015**	**October 2015**
Annual Auction! See page 21!	Palomar Amateur Radio Club board meeting at 7:00pm at Poway Fire Station.	3-4 SD Maker Faire 15-18 JOTA+Microwave Update! 24-25 SSB CQWW

Advertisements are free for members

Have items that need to find a new home? Advertise here! Send your ads to scope@palomararc.org





PALOMAR AMATEUR RADIO CLUB INC.
Since 1936
W6NWG
San Diego County, Ca

Club Members ONLY!
PARC has a tube bank that includes many 6 & 12 volt receiving tubes (and some transmitting types) for use by club members to repair their own personal equipment. Not for commercial use or resale. If we have your requests, we will pre-check the tubes and deliver them to you at the next club meeting.

Contact John WB6IQS WB6IQS@att.net

Helpful DX Tools!

Howard Groveman has provided a link to the websites he talked about in the August general meeting. Check out the list of links here:

http://qsl.net/w6hdg/DXTools.html

Please support our advertisers. Their support of the club is vital.

{special} THANKS to our sponsors

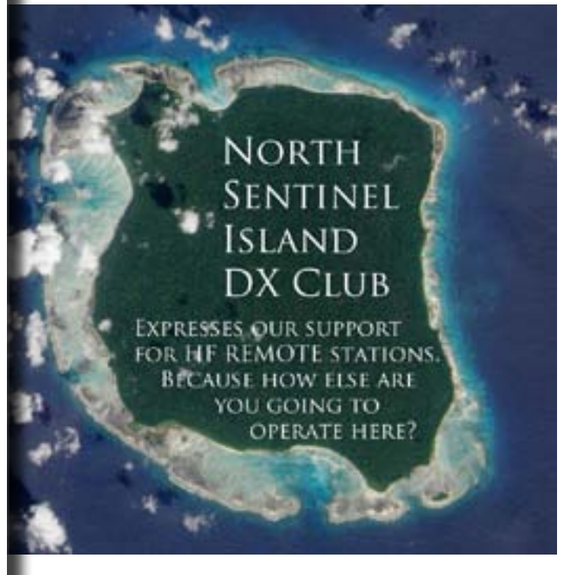
Club HF Remote Station? Proposal Time!

Current status: PARC has obtained 501(c)(3) status, and we have begun putting our HF remote station proposal in writing. This is an exciting time! We expect to complete our proposal by January 2016.

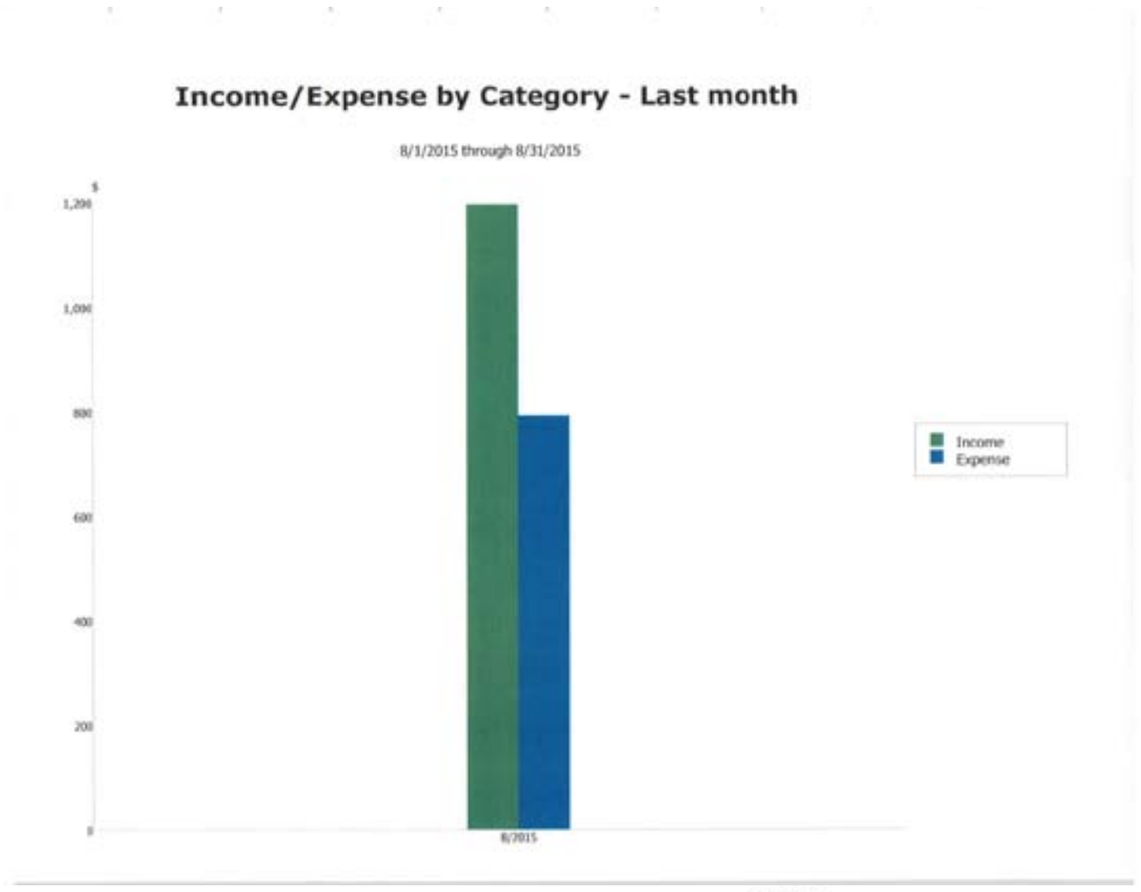
If you would be interested in helping write a club remote HF station proposal for Palomar Mountain, then please join up by writing me at scope@palomararc.org and I'll add you to the mailing list!

Mailing list archive located at http://palomararc.org/pipermail/hfremote/

This special interest group for HF remote will write a proposal for the Palomar Amateur Radio Club board of directors to vote on. If the vote is successful, then fundraising will begin immediately.



Club Financial Update



Category Description	8/1/2015-8/31/2015
INCOME	
Donations	140.00
Dues	906.00
Rentals	150.00
TOTAL INCOME	**1,196.00**
EXPENSES	
Field Day Expns	112.69
Operating Day	219.20
Rptr Electric	104.73
Rptr Maint	231.06
Rptr Phone	30.26
TOWER TRAILER	95.00
TOTAL EXPENSES	**792.94**
OVERALL TOTAL	**403.06**

4 A Protocol for Leibowitz; or, Booklegging by HF in the Age of Safe Æther

by Travis Goodspeed and Muur P.

Howdy y'all!

Today we'll discuss overloading of protocols for digital radio. These tricks can be used to hide data, exfiltrate it, watermark it, and so on. The nifty thing about these tricks is that they show how modulation and encoding of digital radio work, and how receivers for it are built, from really simple protocols like the amateur radio PSK31 and RTTY to complex ones like 802.11, 802.15.4, Bluetooth, etc.

We'll start with narrow-band protocols that you can play with at audio frequencies. So if you don't have an amateur license and a shortwave transceiver, you can use your sound card to do most of the work and run an audio cable between two laptops to send and receive it.[10]

– — – — — – — – — – —

Suppose that sometime in the future, our neighbor Alice lives in an America of modern–day Nehemiah Scudder,[11] whose Youtube preachers and Twitter lynch mobs have made the Internet into a Safe Zone for America's Youth, by disconnecting it from anything unsafe. So Alice's only option to get something unsafe to read is from Booklegger Bob in Canada, by shortwave radio.

But it ain't so easy. President Scudder has directed Eve at the Fair Communications Commission[12] to strictly monitor and brutally enforce radio regulations, defending the principles of Shortwave Neutrality and protecting the youth from microunsafeties.

So Alice and Bob need to make a shortwave radio polyglot, valid in more than one format. Intent on her mission, Eve is listening. So when Alice and Bob's transmissions are sniffed by Scudder's National Safety Agency or overheard by the general public, they must appear to be a popular approved plaintext protocol. It must appear the same on a spectrum waterfall, must decode to a valid message (`CQ CQ CQ de A1ICE A1ICE Pse k`), and nothing may draw undue attention to their communications. Bob, however, is able to find a secret, second meaning.

In this article, we'll introduce you to some of the steganographic tricks they could use, as well as some less stealthy—and more neighborly—ways to combine protocols. We'll start with PSK31 and RTTY, with a bit of CW for good measure. And just to show off, we'll also bring wired Ethernet into the mix, for an exfiltration trick worthy of being shared around campfires![13]

4.1 All You Need Is Sines

Well, not really. But it sure looks that way when you read about radio: sines are everywhere, and you build your signal out of them, using variations in their amplitude, frequency, phase to transmit information.[14] This stands to physical reason, since the sine wave is the basic kind of electromagnetic oscillation we can send through space. Of course, you can add them by putting them on the same wire, and multiply them by applying one signal to the base of a transistor through which the other one travels; you can also feed them through filters that suppress all but an interval of frequencies.

You can see these sines in the signal you receive on the waterfall display of Baudline or FLDigi, which show the incoming signal in the frequency domain by way of the Fourier transform. PSK31 transmissions, for example, will look like nice narrow bands on the waterfall view, which is the point of its design.

The waterfall view is close to how a mathematician would think about signals: all input whatsoever is a bunch of sine waves from all across the spectrum, even noise and all. A perfectly clean sine wave such as a carrier would make a single bright pixel in every line, a single bright 1-pixel stripe scrolling down. That line would expand to a multi-pixel band for a signal that is the carrier being modulated by changing its amplitude, frequency, or phase in any way, with the width of the band being the double of the highest frequency at which the changes are applied.[15]

Of course, the actual construction of digital radio receivers has very little to do with this mathematician's view of the signal. While a mix of ideal sines would neatly fall apart in a perfect Fourier transform, the real transform of sampled signal would have to be discrete, and would present all the interesting problems of aliasing, edge effects, leakage, scalloping, and so on. Thus the actual receiving circuits are specialized for their intended protocols particular kinds of modulation, designed to extract the intended signal's representation and ignore the rest—and therein lies Alice's and Bob's opportunity.

4.2 Related Work

In 2014, Paul Drapeau (KA1OVM) and Brent Dukes released `jt65stego`, a patched version of the JT65 mode that hides data in the error correcting bits.[16,17] The original JT65 by Joe Taylor (K1JT) features frames of 72 bits augmented by 306 error-correcting bits,[18] so Drapeau and Dukes were able to hide encrypted messages by flipping bits that normal radios will flip back. This reduces the odds of successfully decoding the cover message, but they do correct for some errors of the ciphertext.

Our concern in this article is not really stego, though that will be covered. Instead, we'll be looking at which protocols can be combined, embedded, emulated, and smuggled through other protocols. We'll play around with all sorts of crazy combinations, not because these combinations themselves are a secure means of communication, but because we'll be better at designing new means of communication for having thought about them.

4.3 Classic PSK31

PSK31 is best described in an article by Peter Martinez, G3PLX.[19] Here, we'll present a slightly simplified version, ignoring the QPSK extension and parts of the symbol set, so be sure to have a copy of Peter's article when implementing any of these techniques yourself.

This is a Binary Phase Shift Keyed protocol, with 31.25 symbols sent each second. It consumes just a bit more than 60 Hz, allowing for many PSK31 conversations to fit in the bandwidth of a single voice channel.

The PSK31 signal is commonly generated as audio then sent with Upper SideBand (USB) modulation, in which the audio frequency (1 kHz) is upshifted by an RF frequency (28.12 MHz) for transmission. For reception, the same thing happens in reverse, with a USB shortwave receiver downshifting the radio frequencies to the audio range. In older radios, this is performed by an audio cable. More modern radios, such as the Kenwood TS-590, implement a USB Audio Class device that can be run digitally to a nearby computer.

Because many different PSK31 transmissions can fit within the bandwidth of a single voice channel, modern PSK31 decoders such as FLDigi are capable of decoding multiple conversations at once, allowing an operator to monitor them in parallel. These parallel decodings are then contributed to aggregation websites such as PSKReporter that collect and map observations from many different receivers.

4.3.1 Varicode

Instead of ASCII, PSK31 uses a variable-length character encoding scheme called Varicode. This

[10] You could also use loud speakers, but please don't. Pastor Laphroaig reminds us that there is a special level of hell for such people, who will spend Eternity next to those who scratch fingernails on chalk boards.

[11] `unzip pocorgtfo08.pdf ifthisgoeson.txt`

[12] Which some haters call Fundamentalist instead of Fair, but that's unsafe speech. Unsafe speech has consequences, neighbors. You don't want to find out about the consequences, so stay safe!

[13] Campfires are definitely not safe, so enjoy them while they last!

[14] Some combinations are useful, such as amplitude and phase, used, e.g., in DOCSIS; others aren't so useful, such as phase and frequency, because changes in one can't always be told from changes in the other.

[15] This is easy to see for frequency and phase, since these changes are added to the argument of the sine $A \cdot sin(\omega \cdot t + \theta)$, the frequency ω and the phase θ. Seeing this for the amplitude A is a bit trickier, but imagine A to be another sine wave, modulating the carrier. Then we deal with the product of two sines, and this is, by the age-old trigonometric identities $sin(\alpha+\beta) = sin(\alpha)cos(\beta)+cos(\alpha)sin(\beta)$ and $sin(\alpha-\beta) = sin(\alpha)cos(\beta)-cos(\alpha)sin(\beta)$; hence adding these and remembering that the cosine is the sine shifted by $\pi/2$, $sin(\alpha)sin(\beta+\pi/2) = \frac{1}{2}(sin(\alpha+\beta)+sin(\alpha-\beta))$. That is, a product of sines is the arithmetic average of the sines of the sum and the difference of their arguments. If α is the carrier and β is the change, the rainfall diagram will show the band from $\alpha-\beta$ to $\alpha+\beta$, that is 2β-wide.

Seeing this sum and knowing the carrier frequency, one might wonder: can't we make do with just one term of the sum $\alpha+\beta$, and ignore $\alpha-\beta$? Indeed, if one applies a filter to cut the frequencies less than the carrier from the transmitted signal, one can save half the bandwidth and still recover the signal β. This trick is known as the Upper Side Band, and it used for the actual digital radio transmissions.

[16] `https://github.com/pdogg/jt65stego`

[17] Steganography in Commonly Used HF Protocols, Drapeau and Dukes, Defcon 22

[18] `unzip pocorgtfo08.pdf jt65.pdf`

[19] `unzip pocorgtfo08.pdf psk31.pdf`

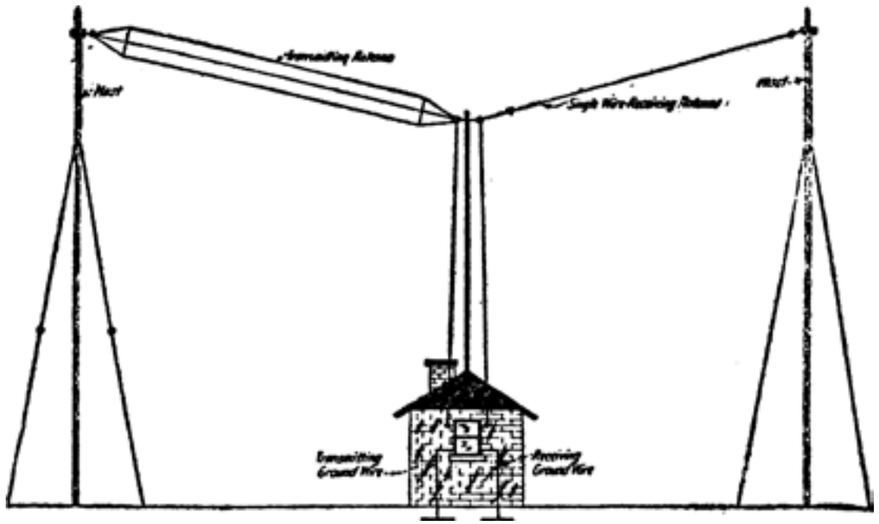
character set features many of the familiar ASCII characters, but they are rearranged so that the most common characters require the fewest bits. For example, the letter `e` is encoded as `11`, using two bits instead of the eight (or seven) that it would consume in ASCII. Lowercase letters are generally shorter than upper case letters, with uncommon control characters taking the most bits.

A partial Varicode alphabet is shown in Figure 2. Additionally, an idle of at least two `0` bits is required between Varicode characters. No character begins or ends with a `0`, and for clock recovery reasons, there will never be a string of more than six `1` bits in a row.

4.3.2 Encoding

To encode a message, letters are converted to bits through the Varicode table, delimited by `00` to keep them distinct. As PSK31 is designed for live use by a human operator in real time, any number of zeroes may be appended. That is, "`e e`" can be rendered to `110010011`, `110000010011`, or `1100100011`; there is no difference in meaning, only transmission time.

PSK31 encodes the bit `1` as a continuous carrier and the bit `0` as a carrier phase reversal. So the sequence `11111111` is a boring old carrier wave, no different from holding a Morse key for a quarter-second, while `00000000` is a carrier that inverts its phase every 31.25 ms.



So what's a phase reversal? It just means that what used be the peak of the wave is now a trough, and what used to be the trough is now a peak.

4.3.3 Decoding

As described in Martinez' PSK31 article, a receiver first uses a narrow bandpass filter to select just one PSK31 signal.

It then multiplies that signal with a time-delayed version of itself to extract the bits. The output will be negative when the signal reverses polarity, and positive when it does not.

Once the bits are in hand, the receiver splits them into Varicode characters. A character begins as the first `1` after at least two zeroes, and a character ends as the last `1` before two or more zeroes. After the characters are split apart, they are parsed by a lookup table to produce ASCII.

4.4 PSK31 Stego

4.4.1 Extending the Varicode Character Set

G3PLX's original article contains a second part, in which he notes that his original protocol provides no support for extended characters, such as the British symbol for pounds sterling, £. Wishing to add such characters, but not to break compatibility, he noted that the longest legal Varicode character was ten

Figure 1: PSKReporter, a Service for Monitoring PSK31

bits long. Anything longer was ignored by the receiver as a damaged and unrecoverable character, so PSK31 uses those long sequences for extended characters.

Reviewing the source code of a few PSK31 decoders, we find that Varicode still has not defined anything with more than twelve bits. By prefixing the character Alice truly intends to send with a pattern such as `101101011011`, she can hide special characters within her message. To decode the hidden message, Bob will simply cut that sequence from any abnormally long character.

4.4.2 Hiding in Idle Lengths

PSK31 requires *at least* two `0` bits between characters, but it doesn't specify an exact limit. It's not terribly uncommon to see forgotten transmitters spewing limitless streams of zeroes into the ether as their operators sit idle, never typing a character that would result in a zero. Alice can abuse this to hide extra information by encoding data in the variable gap between characters.

For an example, Alice might place the minimal pair of zero bits (`00`) between characters to indicate a zero while a triplet (`000`) indicates a one.

4.4.3 Extending the Symbol Set

In its classic incarnation, PSK31 uses Binary Phase Shift Keying (BPSK), which means that the phase flips 180 degrees. This is sometimes called BPSK31, to distinguish it from a later variant, QPSK31, which uses Quadrature Phase Shift Keying (QPSK).

11101	LF	1011	a	1111101	A
11111	CR	1011111	b	11101011	B
1	SP	101111	c	10101101	C
10110111	0	101101	d	10110101	D
10111101	1	11	e	1110111	E
11101101	2	111101	f	11011011	F
11111111	3	1011011	g	11111101	G
101110111	4	101011	h	101010101	H
101011011	5	1101	i	1111111	I
101101011	6	111101011	j	111111101	J
110101101	7	10111111	k	101111101	K
110101011	8	11011	l	11010111	L
110110111	9	111011	m	10111011	M
		1111	n	11011101	N
		111	o	10101011	O
		111111	p	11010101	P
		110111111	q	111011101	Q
		10101	r	10101111	R
		10111	s	1101111	S
		101	t	1101101	T
		110111	u	101010111	U
		1111011	v	110110101	V
		1101011	w	101011101	W
		11011111	x	101110101	X
		1011101	y	101111011	Y
		111010101	z	1010101101	Z

Figure 2: Partial PSK31 Varicode Alphabet

QPSK performs phase changes in multiples of 90 degrees, providing G3PLX extra symbol space to perform error correction.

Alice can use the same trick to form a polyglot with BPSK31, but this presents a number of signal processing challenges. Simply using the 90-degree shifts of QPSK31 would be a bit of an indiscretion, as BPSK interpreters would have wildly varying interpretations of the message, often decoding the hidden bits to visible junk characters.

Using a terribly small shift is a tempting idea, as Alice's use of balanced 170 and 190 degree transitions might be rounded out to 180 degrees by the receiver. Unfortunately, this would require *extremely* stable and well tuned radio equipment, giving Bob as much trouble receiving the signal as Eve is supposed to have!

Instead of adding additional phases to BPSK31, we propose instead that the error correction of QPSK31 be abused to encode additional bits. Alice can encode data by *intentionally inserting errors* in a QPSK31 bitstream, relying upon Eve's receiver to remove them by error correction. Bob's receiver, by contrast, would know that the error bits are where the data really is.

4.5 Classic RTTY (ITA2)

RTTY—pronounced "Ritty"—is a radio extension of military teletypewriters that has been in use since the early thirties. It consists of five-bit letters, using shifts to implement uppercase letters and foreign alphabets. Although implementation details vary, most amateur stations use 45 baud, 170Hz shift, 1 start bit, 2 stop bits, and 5 character bits. The higher frequency is a mark (one), while the lower frequency is a space (zero).

As more digital protocols other than CW and RTTY weren't legalized until the eighties, all sorts of clever tricks were thought up. Figure 4 shows RTTY artwork from W2PSU's article in the September 1977 issue of 73 Magazine. Lacking computerized storage and cheap audio cassettes, it was the style at the time to store long stretches of paper tape as rolls in pie tins, with taped labels on the sides.

Figure 6 describes Western Union's ITA2 alphabet used by RTTY, which is often—if imprecisely—called Baudot Code. In that figure, `1` indicates a high-frequency mark while `2` indicates a low-frequency space. Note that these letters are sent almost like a UART, least-significant-bit first with one start bit and two stop bits.

4.6 Some Ditties in RTTY

4.6.1 Differing Diddles

Unlike a traditional UART, RTTY sends an idle character—colloquially known as a Diddle—of five marks when no data is available. This is done to prevent the receiver from becoming desynchronized, but it isn't strictly mandatory. By not sending the diddle character (`11111`) when idle, the mark bit's frequency can be left idle for a bit, encoding extra information.

Additionally, there are not one but *two* possible diddle characters! Traditionally the idle is filled with `11111`, which means `Shift to Letters`, so the transmitter is just repeatedly telling the receiver that the next character will be a letter. You could also send `11011`, which means `Shift to Figures`. Sending it repeatedly also has no effect, and jumping between these two diddle characters will give you a side-channel for communication which won't appear in normal RTTY receivers. As an added benefit, it is visually less conspicuous than causing the right channel of your RTTY broadcast to briefly disap-

BPSK	10101101	00	111011101	000	1	00	10101101	000	111011101	00	1	00
PSK31	C		Q		[SP]		C		Q		[SP]	
Idle		0		1		0		1		0		
BPSK	101101	00	11	000	1	00	1111101	000	10111101	00	1111111	00
PSK31	d		e		[SP]		A		1		I	
Idle		0		1		0		1		0		0
BPSK	10101101	00	1110111	0	0	0	0	0	0	0	0	0
PSK31	C		E									
Idle		0										

Figure 3: `010100101000` Hidden in PSK31 Idle Bits

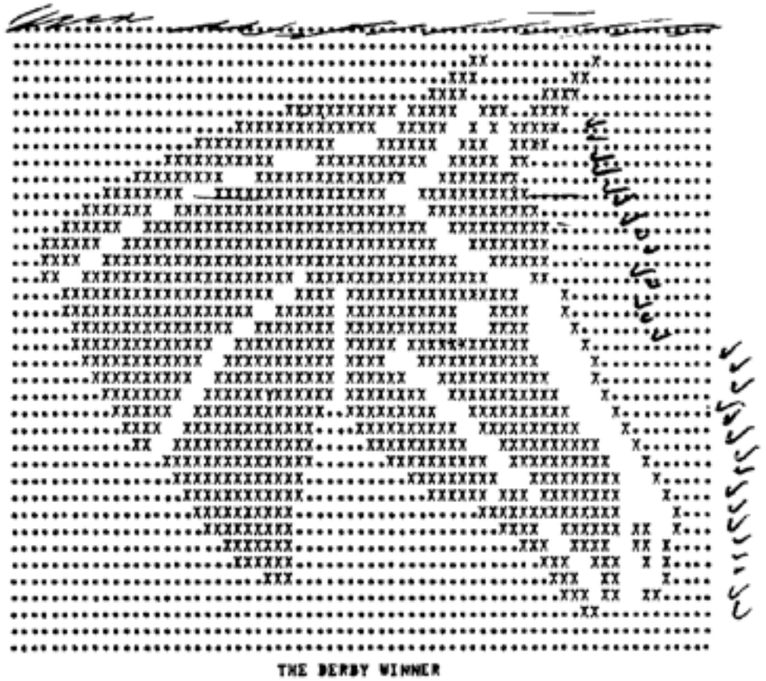


Figure 4: RTTY Art of Seattle Slew from the mid 1970's

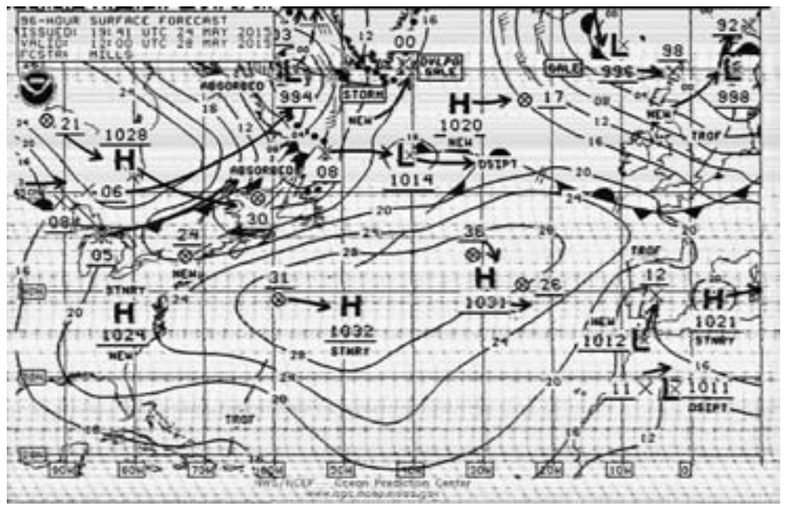


Figure 5: Weather Fax

	Letter	Figure		Letter	Figure
00000	Null	Null	11010	G	&
00100	Space	Space	10100	H	#
10111	Q	1	01011	J	’
10011	W	2	01111	K	(
00001	E	3	10010	L	)
01010	R	4	10001	Z	”
10000	T	5	11101	X	/
10101	Y	6	01110	C	:
00111	U	7	11110	V	;
00110	I	8	11001	B	?
11000	O	9	01100	N	,
10110	P	0	11100	M	.
00011	A	–	01000	CR	CR
00101	S	Bell	00010	LF	LF
01001	D	WRU?	11011	FIGS	
01101	F	!	11111		LTRS

Figure 6: RTTY's ITA2 Alphabet

pear!

4.6.2 Stop with the Stop Bits!

RTTY is described in the old UART tradition as `5/N/2`, meaning that it has `5` data bits, `N`o parity bits, and `2` stop bits. There's a cool trick to UARTs that's worth remembering: the transmitter can always have *more* stop bits than the receiver demands, and the receiver can always demand *fewer* stop bits than the transmitter sends.

4.7 Toe Tappin' CW

Carrier Wave (CW) modulation—better known as Morse code—was the first widely deployed digital mode to replace spark-gap transmitters. Designed for a human operator to manually use, CW is a perfect choice for easy polyglots.

As a quick review, CW consists of dots and dashes. A dash is three times as long as a dot. The off-time between elements of a letter is as long as a dot, and the off-time between letters in a word is as long as a dash. The off-time between words is seven times as long as a dot, or a bit more than twice as long as a dash.

4.7.1 QRSS

While other protocols have standard data rates, Morse relies on the recipient to adjust to the rate of the transmitter. Operators often find themselves unable to keep up with an expert or impatiently waiting on a station that transmits slowly, so shorthand was developed to ask the other side to change rate. `QRQ` requests that the other side transmit more quickly, and `QRS` requests that the other side slow down.

QRSS is a variant of CW in which the message is sent very, *very* slowly. Rather than a dot lasting a fraction of a second, it might last as long as a minute! A receiver can then take a recording of a very weak signal, slow down the recording, and visually observe the signal to determine its meaning.

While protocols such as RTTY and PSK31 don't take kindly to the sorts of frequent interruptions that normal CW would impart, these protocols can easily produce QRSS transmissions that are legible by slowing down recordings. For example, Alice might send "`A1BOB A1BOB de A1ICE`" for a dot and "`A1BOB A1BOB de A1ICE. A1BOB A1BOB de A1ICE. A1BOB A1BOB de A1ICE.`" for a dash.

This is of course a bit easy to recognize from a waterfall, but it might be a fun way to meet your neighbors!

4.7.2 From Ethernet to Æther with Madeline

In a row house in Philly
that was covered with vines
Was an Ethernet network
in four twisted lines
In four twisted lines
they ran to the laundry
And to the satellite dish
and to the pantry
The twists ended too soon
and ceased to align
Interfering with 10 meters
all down the line
The protocol
was Madeline.

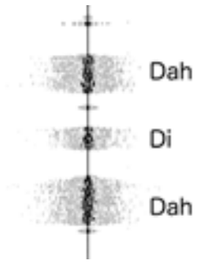
It's clear enough that you could transmit Morse code through Wifi by sending bursts of traffic, but what about wired Ethernet?

Some folks are very particular when wiring CAT5e cable, ensuring that the twisted pairs are untwisted at the last possible position before the connector. Other folks—such as your neighborly authors—are far less particular in their wiring, and when the wiring is performed poorly, interference is observed near 28.121 MHz!

Still better, the interference varies with traffic! When the network is idle, the interference appears as a nice thin carrier wave. When the network is busy, the interference grows to be nearly four hundred Hertz wide.

The following is a letter of Morse code transmitted from (poorly) wired Ethernet to the 10-meter band through what we are calling the Madeline protocol. This transmission isn't strong enough to carry very far, but the Baudline-generated waterfall in that figure was recorded from outside of a real house, with a signal generated by a real Ethernet network. The recording was made by an Upper SideBand receiver tuned to 28.120 MHz.[20] The narrow-band signal at 28.121 MHz becomes wide whenever lots of traffic goes across the wired network; in this case, from activity on a VNC session.

[20] `unzip pocorgtfo08.pdf madelinek.wav`



4.8 Patching FLDigi

All of this high-falutin' theorizin' don't do a lick of good without some software to back it up. Supposing that Alice is a modern unix programmer, but that Bob hasn't written code for anything more modern than a Commodore 64, Alice will need to provide him with a GUI application that easily interfaces with his radio.

The most direct route for this is to patch FLDigi, a popular open source application for digital communication over ham radio with a live operator. Internally, FLDigi implements softmodems for CW, PSK31, RTTY, WEFAX, and several other protocols.

4.9 Part 97; or, Don't be a Jerk!

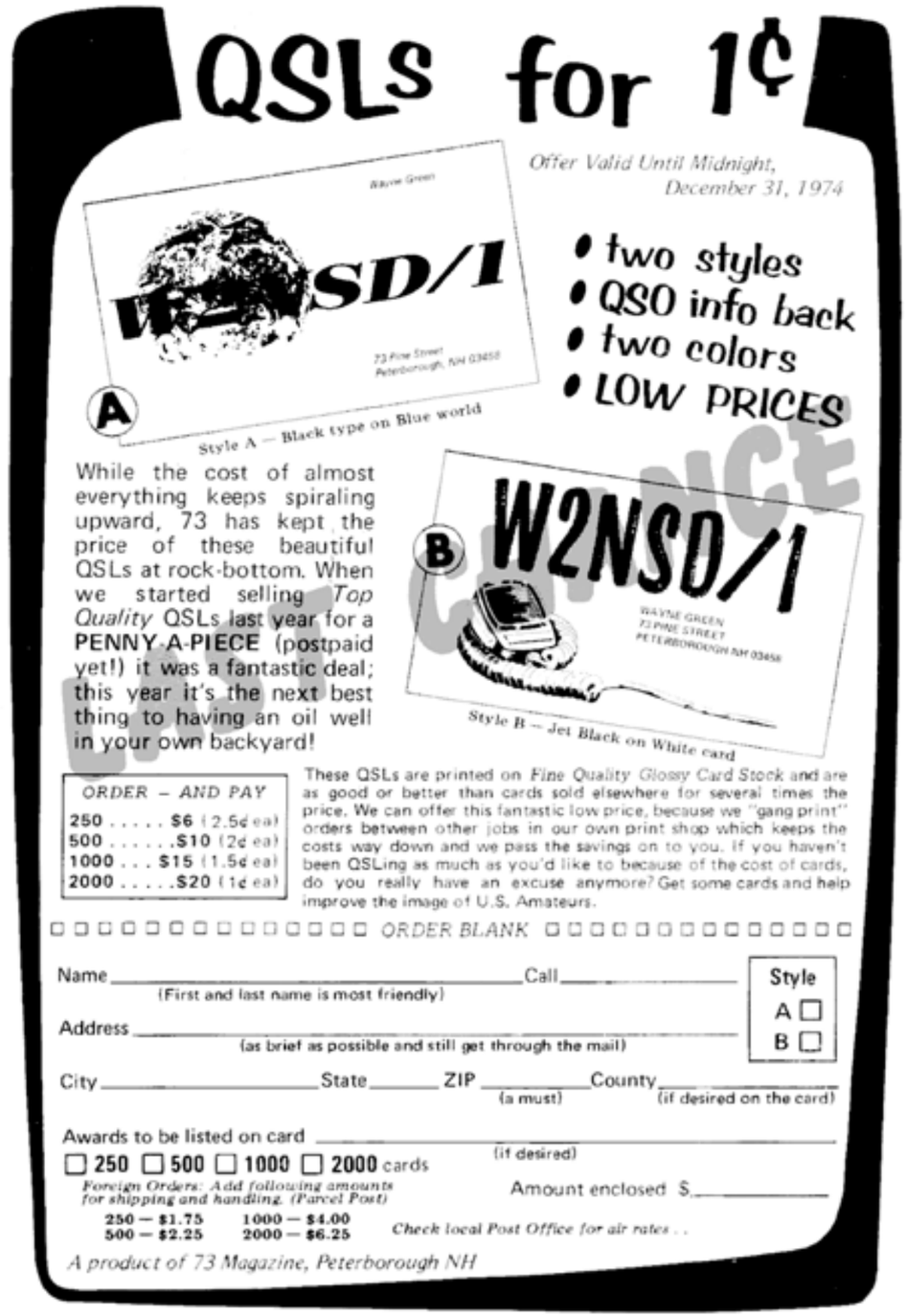
Be aware that in general, it's both illegal and immoral to be a jerk on the amateur bands. Interference is forbidden in amateur radio, not because jamming research is bad, but because it's rude to stomp on someone else's transmission. Cryptography is forbidden in amateur radio, not because of any evil conspiracy to destroy privacy, but because cryptography makes a transmission opaque, preventing newcomers from joining the conversation.

So for those of you who do not live in Nehemiah Scudder's oppressive theocracy, please be so kind as to keep your polyglot messages unencrypted. Make a fox hunt of sorts out of your protocol experimentation, with the surface PSK31 message advertising your callsign along with the name and parameters of your real protocol.

– – – – – – – – – – – –

We hope that this article has taught you a little about radio and signal processing. Get an amateur license, build a station, and start experimenting with new protocols on the friendly airwaves.

73's from Appalachia,
—Travis and Muur



Amateur Radio at DEFCON 23

by Michelle W5NYV

DEFCON 23 was held August 6-9 in Paris and Bally's hotels in Las Vegas, Nevada. This four-day event is a seething mass of information overload, activities, talks, contests, villages, workshops, vendors, demonstrations, proofs of concept, parties, pranks, music, and networking. An estimated 20,000 people attended DEFCON 23.

To kick off the event at 10am Thursday August 6th, a track of talks called DEFCON 101 was presented. One of these was "Introduction to SDR and the Wireless Village". Presented by DaKahuna and satanklawz, two hams "keeping it legal", the talk introduced the current crop of commonly encountered SDRs with an emphasis on how not to fail in efforts to get one on the air. Speaking to an audience that they had to assume might have limited RF experience, they underlined the importance of having an appropriate antenna.

"Success depends on antennas and filters. Do not transmit with mismatched antenna system. You will cry," explained DaKahuna. Satanklawz nodded sagely. Other good advice included picking he right tool for the job. To illustrate, the pair discussed BladeRF, HackRF, USRP, and RTL-SDR, comparing and contrasting the capabilities and strengths of each type of SDR.

Satellite, EME, packet, RTTY, IRLP, Morse code, and how all these ham activities apply directly to expanding a security researcher's signal intelligence capabilities were discussed in a conversational and accessible style.

"Software LIES to you. There are harmonics!" satanklawz thundered from the podium. He counseled the full-to-capacity crowd to "know your antenna" and learn propagation for the frequencies of interest, warning that signals can experience diffraction, reflection, refraction, and multipath. All of this was old hat for some hams in the audience, but the DEFCON crowd has many brand-now "I have my license, now what?" hams as well as people who have never heard of ham radio or signal intelligence before.

The pair recommended gqrx and SDR# for browsing spectrum on SDRs. They recommended GnuRadio as a decoding platform. Baudline was mentioned as a non-GPL albeit quirky package that deserved a look.

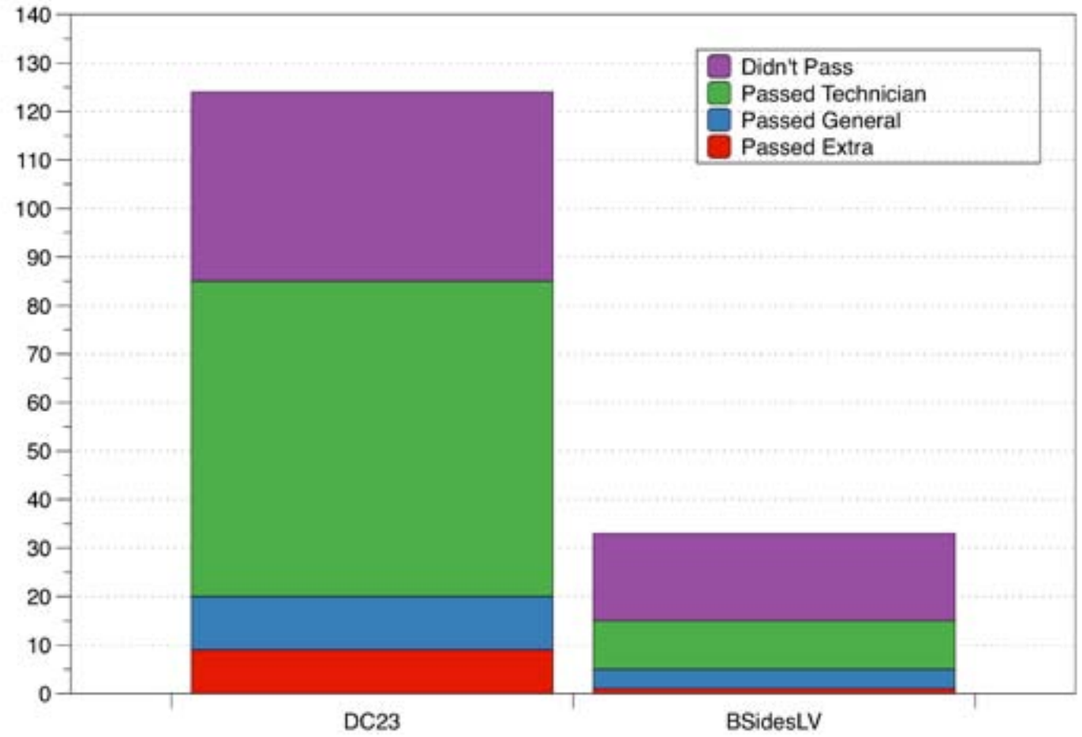
They warned about SDR lab problems like antennas, lightning, static, noise, clocks and drift. They explained that connectors were sometimes "super sucky", and to be aware that different cables behaved very differently at different frequencies. They warned that the cheaper SDRs don't have ESD protection, and that a reading of Naval RFI Handbook would be highly educational. They shared stories of battling the unintended consequences of unshielded power receptacles, galvanic corrosion, frequency drift due to heating, and noisy clocks.

They then discussed another aspect of DEFCON where amateur radio loomed large – the Wireless Village. Villages at DEFCON are theme camps where specific activities, lecture series, workshops, contests, hands-on training, and interactive exhibits can be found.

Set aside in their own spaces, Villages provide a specific subject matter experience. Wireless Village was, as you might have guessed, focused on wireless technologies. Other Villages included Crypto & Privacy, Hardware Hacking, Lockpick, Packet Hacking, Tamper Evident, Car Hacking, Bio Hacking, Social Engineering, Data, ICS, and Internet of Things. Some of these villages hosted their own contests.

Tamper Evident village has a contest where you take apart tamper evident packaging. The challenge is to open a series of packages that are each inside the other, from a large box sealed with tamper evident tape down to a small tamper evident envelope. The final envelope contains some sort of evidence that proves you've reached the most interior package. Then, you have to put them all back together without revealing that they've been opened. If you have a Uline catalog, pretty much every product in the tamper evident section is represented. The winners are the ones where the evaluation team cannot tell the packages have been opened.

Wireless Village hosted its own lecture series, had all sorts of SDRs available for experimentation, held a wireless capture the flag contest, and also supported the DEFCON amateur radio exam session. For DEFCON 23, the exam session was open all day long on Saturday. Exams were available as a reservation or one could walk in. Results are summarized



in the chart. For comparison, the ham radio exams from BSides Las Vegas are also included. BSides is a series of hacker conferences that draw a very similar crowd to DEFCON. They are usually much smaller. It's very exciting to see so much licensing activity within the technical communities of DEFCON and BSides.

All three of my children attempted the amateur radio exam during the DEFCON test session. My son, KK6OOZ, attempted to upgrade to a General license. My two daughters went for their Technician. Unfortunately, none of them passed this time around, but their interest was certainly revitalized and the spark has only grown since our 5 days in Vegas. My son attended the SDR 101 talk and greatly enjoyed it. My son and I attended the all-day Raspberry Pi Workshop on Saturday, where we had an incredibly good time learning the Raspberry Pi ropes.

Here's the biographies of the presenters for the SDR and Wireless Village talk.

By day DaKahuna works for a small defense contractor as a consultant to large government agencies providing critical reviews of customer organizations compliance with Federal Information Systems Information Security Act (FISMA) requirements, effectiveness of their implementation of National Institute for Science and Technology (NIST) Special Publication requirements, cyber security policies, cyber security program plans, and governmental standards and guidance. By night he enjoys roaming the airwaves, be it the amateur radio bands or wireless networks. He is a father of two, grandfather to three, 24 year Navy veteran communicator, holder of an amateur radio Extra Class license and a staunch supporter and exerciser of his 2nd Amendment rights who enjoys shooting targets out to 1200 yards.

Satanklawz has been in the information security realm for 15 years. He built and sold a wireless ISP, worked info sec in the financial services industry and now is a public servant of sorts. His hobbies and interests have always involved radio in some sort of fashion. When he has spare time, he is completing his PhD, teaches, create mischief, and is working on his dad jokes.

Amateur Radio at Burning Man - SDR

RTL-SDR at Burning Man

Spying on Planes!

By Michelle W5NYV

After learning about RTL-SDR at the "Introduction to SDR and the Wireless Village" talk given at DEFCON 23, I bought one in the DEFCON vendor area. It was $20 and included a small whip antenna. The size of a pack of gum, it could easily fit in a pocket. I decided to take it to Burning Man and track airplanes.

At DEFCON 22, I'd learned about ADS-B. Automatic Dependent Surveillance Broadcast or ADS-B is the latest advance in airspace surveillance. ADS-B uses a Trig transponder, typically combined with a GPS, to transmit position of the aircraft to both ground controllers and also directly to other aircraft. Essentially, ADS-B replaces radar. It has several advantages over radar, including working over "non-radar" areas, allowing more aircraft to operate in a given airspace and enabling direct routing. There is some evidence that it has improved flight safety in the US.

However, since ADS-B can be turned on or off, a plane could theoretically hide from the public. Without radar, an uncooperative plane would seem to be a big problem.

In time ADS-B is expected to supersede existing surface-based radar systems. Radar is expensive and has some limitations that ADS-B gets around, such as geographical limitations, false returns, and delays. ADS-B is much cheaper than a radar installation.

According to Trig Avionics, an ADS-B systems supplier, "ADS-B surveillance technology that does not rely upon ground controllers was first trialled in Alaska. This region was selected as an early proving ground for ADS-B and associated FAA 'Next Gen' technologies. This was due to the significant commercial aviation accident rate suffered in this harsh operating environment. Aircraft were fitted with ADS-B, GPS moving maps and improved communications to enhance safety. In South West Alaska ADS-B (combined with these other initiatives) helped to reduce fatal accidents by 47%."

Phil Karn and Franklin Antonio had both set up ADS-B monitoring systems at home using Raspberry Pis. I decided to set up the RTL-SDR at burning man for ADS-B. To make the challenge a bit harder, I only downloaded GnuRadio and gqrx on the macbook before leaving. I didn't look up or read anything about ADS-B. I'd figure it out on the relatively remote dry lakebed home to Black Rock City.

This self-imposed limit proved to be a somewhat silly idea. I rapidly figured out how to connect the RTL-SDR to the macbook and successfully received BMIR, Burning Man Information Radio, on 94.5 FM. I then successfully demodulated APRS from the other Burner hams that were puttering around the city. I then hunted down FRS communications between camps and volunteers. All were accomplished using gqrx out of the box. However, I didn't have a demodulator for ADS-B. I needed yet more software. It turned out the right tool for the job was a package on github called dump1090 (https://github.com/antirez/dump1090).

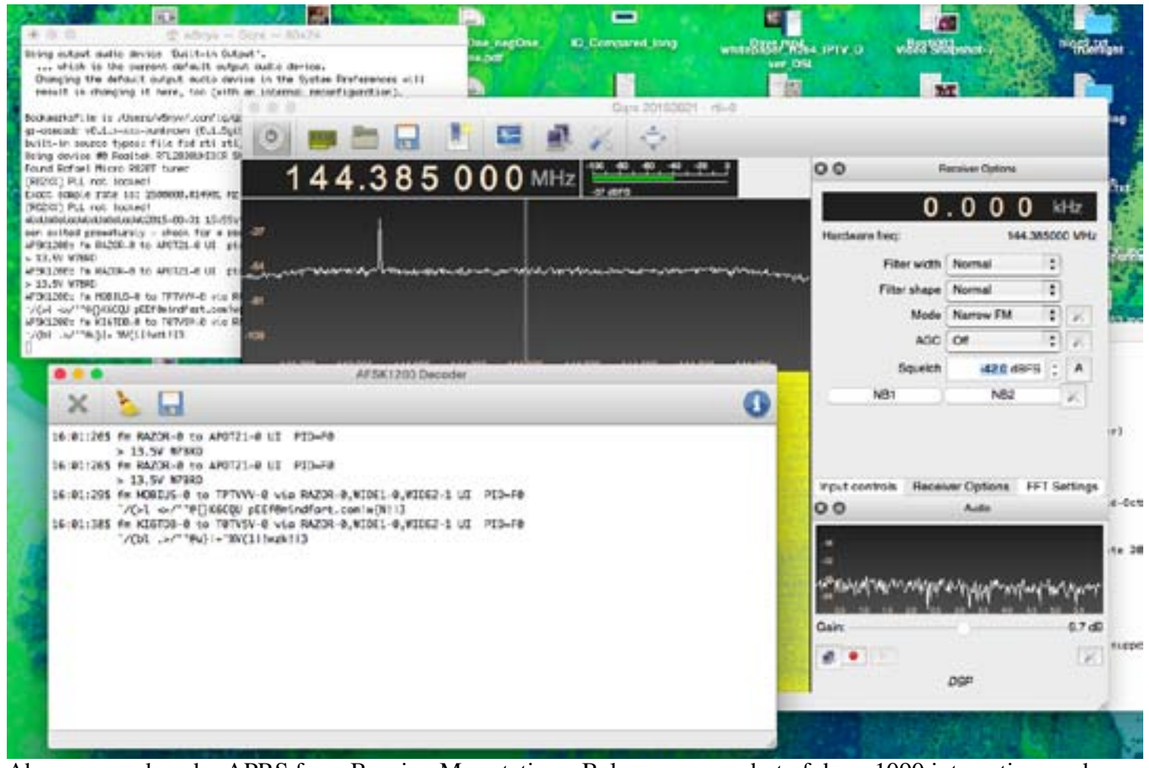
Normally, there is no data service on the playa. However, this year, the very thinnest connection over cellular could be had if you were patient and opportunistic. Using the command line on the macbook, I tried over and over until, during a moment of connectivity, I was able to grab the repository and clone it on the computer.

I then followed the simple instructions to build dump1090. I ran it in interactive mode, and there they were. Airplanes! The 1090 stands for the frequency used by ADS-B, which is (as you've probably guessed) 1090MHz.

I could see both low-altitude local traffic coming in and out of Burning Man's airport, as well as commercial aircraft that were much higher in altitude. I took the laptop, SDR, and antenna outside and put the antenna on the hood of the truck. The mag-mount whip's antenna performance dramatically improved. I took a screenshot and declared victory.

I greatly enjoyed watching the aircraft come and go over the next few days. Although I didn't have enough of a connection to Google maps to do this, a feature of the dump1090 is that it will draw the planes on the map for you, with their headings and tracks noted.

This experience should illustrate one of the great advantages of SDRs. With one tiny $20 radio and a small whip antenna, I was able to receive a commercial broadcast station, decode APRS packets from my fellow hams, search for and find FRS communications, and spy on aircraft skulking around Burning Man, all in the space of about an hour. With a wide variety of other software packages, or with software I write myself, the RTL-SDR can do an enormous additional amount of receiving. Reconfiguring a radio on the fly is a remarkable and thrilling capability to have!



Above, gqrx decodes APRS from Burning Man stations. Below, a screenshot of dump1090 interactive mode, and the station itself set up on the hood of the truck. The SDR is in the USB port on the righthand side of the laptop.

Source vs. Process

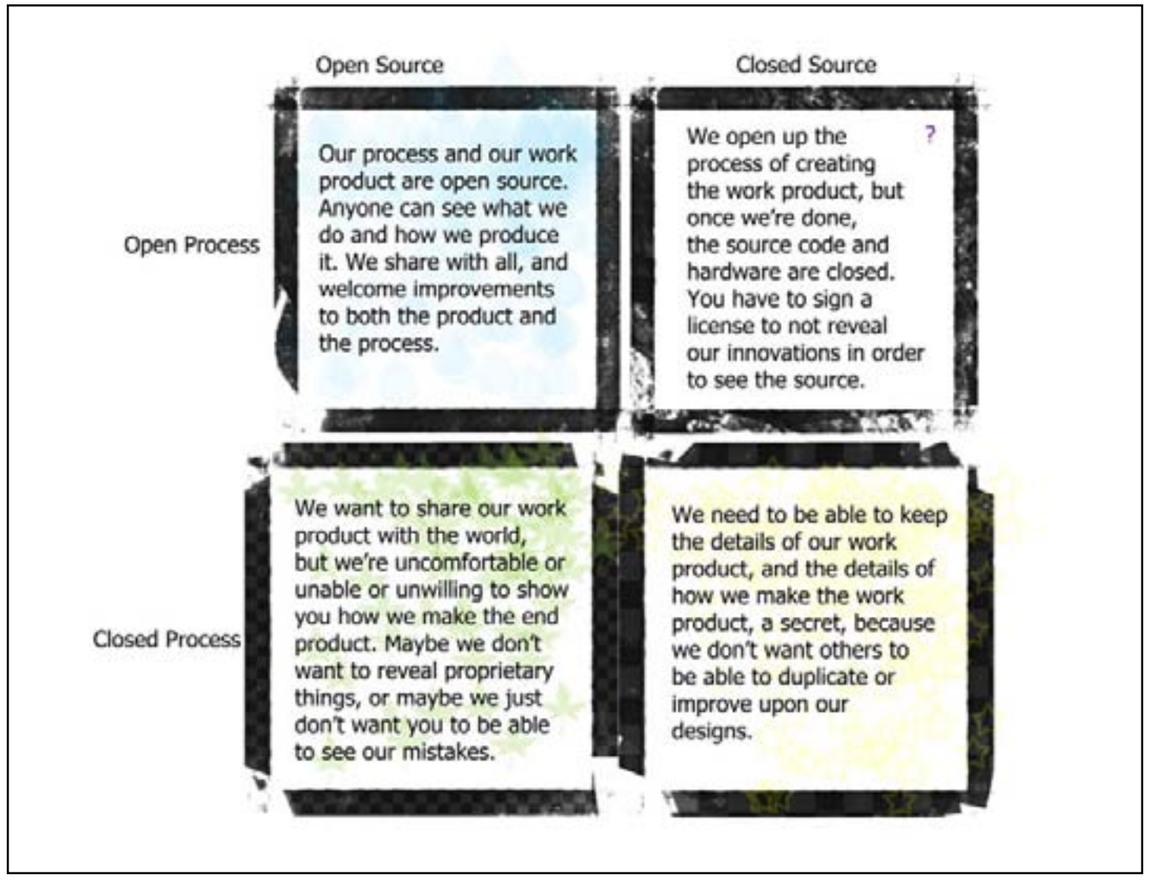
There are many ways to structure and define collaborative work. If you work on projects with other people, where does yours fall in the chart below?

Open source projects currently get a lot of press. Usually, open source means that the source code or schematics are freely published, instead of being held secret. However, the work product itself isn't the whole story. The process of creating the work can be either open or closed or somewhere in between. Looking at both dimensions, the work product along with the work process, provides a more complex view of the charactistics of a project.

If you're drawn to open source projects, it's worth digging deeper into how things are structured in order to avoid any communications problems along the way.

While many amateur radio projects are open source, some are not (e.g. Winlink). Some are open source, but closed process (e.g. some AMSAT projects). The reaons for this vary, but a thumbnail sketch of possible mindsets for each quadrant is summarized below.

Text and graphic by Michelle W5NYV.



Palomar Amateur Radio Club Auction
OCTOBER 7th. 2015

ALL ARE INVITED

COME AND GET YOUR EARLY HALLOWEEN HAM CANDY!!

DETAILS

PLACE: Carlsbad Safety Center
2560 Orion Way
Carlsbad
TIME:
VENDOR SETUP: 6:00 PM
BUYER INSPECTION: 6:30 PM
AUCTION START: 7:00 PM

TALK IN
146.730 MHz
PL: 107.2
DIGITAL OR ANALOG

Arduino + Wifi = Particle Development Board

Arduino, Raspberry Pi, and other development boards have taken the amateur radio world by storm. Being able to experiment with small microcontrollers has never been easier.

Another entrant into the world of embedded development kits is Particle. Particle recently introduced the Photon.

The Photon is an Arduino plus Wifi. The video above shows what's inside the Photon development kit. Notice that the processor is already installed on a breadboard, and that a paper label shows exactly where to place components for the first experiment. Learning the basics is easy and fun.

The Electron, also by Particle, is an Arduino plus cellular. Remote sensing is the intended market.

August - September 2015 Work Party Reports

On 13 September 2015, a work party was held at the PARC repeater site. Dennis KD6TUJ and Richard KJ6WUY worked on the exteriors of some of the buildings in order to apply a layer of green paint over the brilliant green primer paint previously applied.

John Kuivinen WB6IQS and Mark Raptis KF6WTN repaired two aspects of the 146.700 Packet Repeater.

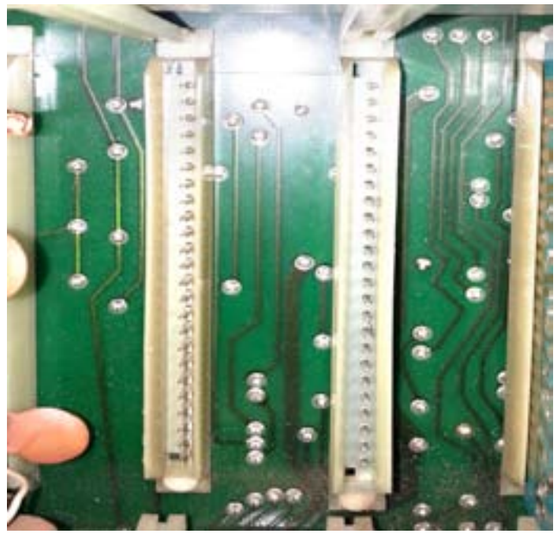
John, WB6IQS Reports:

Report on 146.700 activities:
Update, Sept. 7, 2015

Rich, NI6H and John, WB6IQS

Rich, Mark Raptis and I have been fighting an intermittent problem for some months and finally I believe that we have nailed it.

After repairing a bad antenna connection last week (See Bigfoot on the Mountain page 26) another old problem again reappeared. Today when we first got to the mountain the PTT (Push to Talk) test button was not working on the Station Control Module but after wiggling it in the socket it began to work. This behavior has been an on-going problem for some months. The card was seated in the card cage, but never felt really "tight" and as secure as the other cards had been. I was unable to push it any further into the socket without fear of breaking something.



On close visual inspection from the front of the motherboard the problem became apparent. A 24 socket vertical plastic pin guide rail was at a cockeyed angle and prohibiting the card from becoming fully seated.

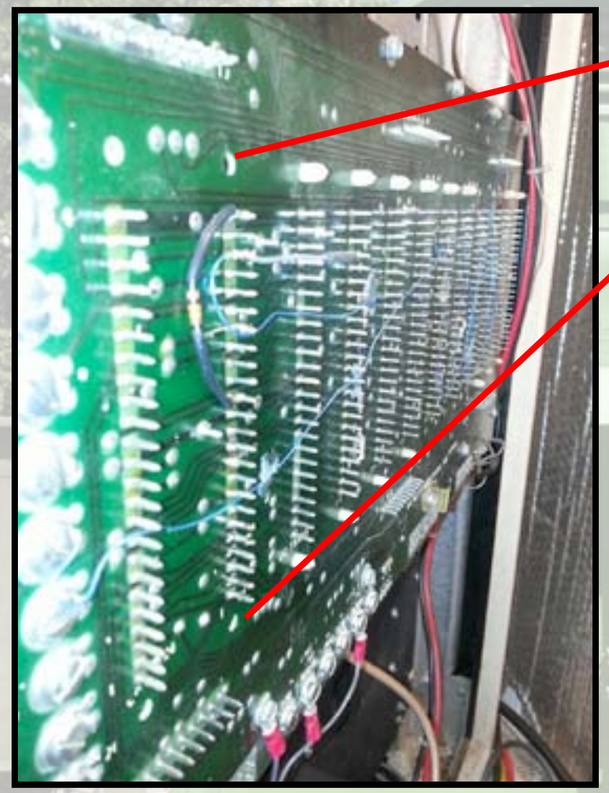
I needed new plastic hardware snap locks to reseat the pin guide but none were immediately available. Removing other cards in the rack allowed me to hold the pin guide in place when seating the board fully into the rack. I then replaced all the other cards to finish the repair.

Hopefully this is the last nail in the coffin of this on-going problem. When installing PCBs in older equipment you never want to just force something into place, your equipment may not survive the efforts.

Top pins are extended about 0.375” out from the plastic guide rail, the bottom pin are only extend about 0.125”.

This 40 year old nylon hardware is very brittle and the snap lock pins are not reliable holders of the pin guide rails. I am going to try to find some replacement motherboard snaps at Frys or through the Internet.

John Kuivinen, Vista, CA
WB6IQS



Broken snap pins that held the pin guide rail (see below for guide rail photo) in place. This allowed the pin guide rail to go out of position.

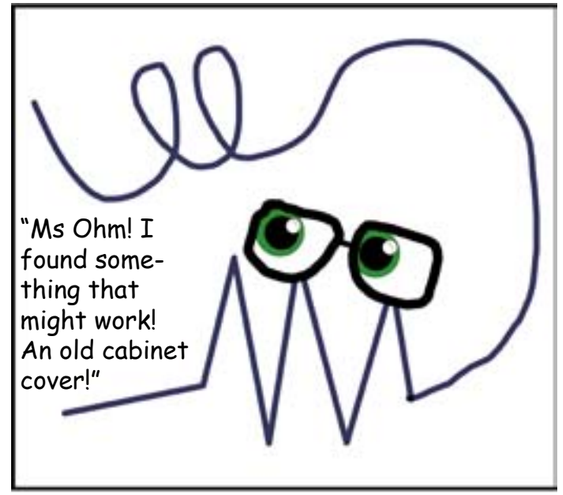
Here’s what a pin guide rail looks like.

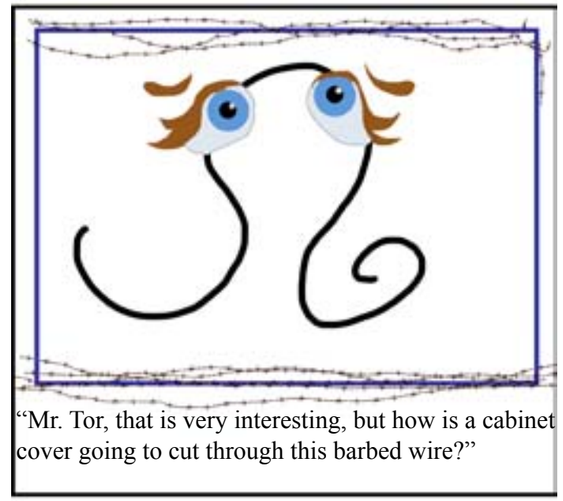
When last we left, Mr. Tor had escaped, but Ms. Ohm was still trapped. Her prison seems to be getting less and less comfortable. Who or what could possibly be behind this nefarious game?

Rear Door Cover: An example of the many years of modifications and “improvements” that were required to allow cables and control wiring to enter the cabinet.

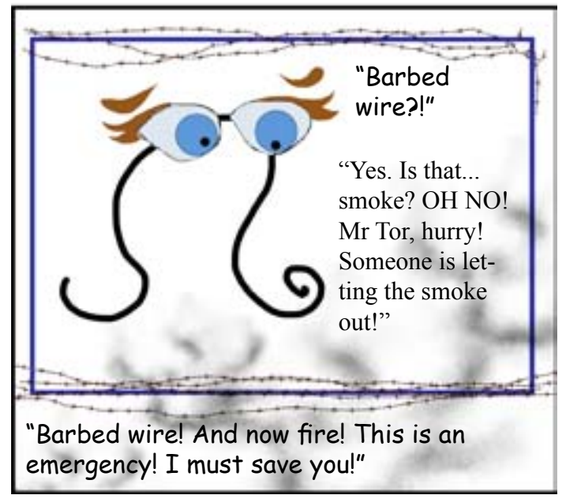
The bottom vents were once similar to the upper right vent. They have been replaced with metal screening using pop rivets.

Sediment in the battery bank. Mark KF6WTN is designing a charge equalizer to head off this problem and extend the life of the battery bank.





“Mr. Tor, that is very interesting, but how is a cabinet cover going to cut through this barbed wire?”



Bigfoot Loose on the Mountain

Repeater Repair 101

John WB6IQS, August 29, 2015

On August 8 at 11 AM (keep that date / time in mind) it was later reported that the 146.700/.100 digital packet repeater was inoperative. However, no one was immediately available to do a work party at the repeater site. Rich, NI6H and I planned on going up early last week but after a number of discussions about what was required Mark Raptis, KF6WTN and I went up today.

Repair Procedures:
Arrived at the site about 11 AM:

First thing was to check the 54 VDC primary input voltages, OK. We then checked the output 13.8 VDC power supply voltages, OK. Dragged out the RF service instruments and warmed them up. Receiver input OK, transmitter power output into the cavities OK. FM deviation on the transmitter checks OK. Hmmmmm?

Checked VSWR before the cavities, shows OK but this is not a true indication since the isolation cavities can mask an antenna problem. We have RF circulators on the repeater's output. A circulator is kind of magnetic diode to RF where RF power can go out but if you have a high VSWR or other repeaters in the area then RF is not returned back to the transmitter. This prevents spurious emissions and cross modulation from the other solid state repeater transmitters at the site. If circulators were not present we would have more "birdies" and mixing products due to the high level of RF (both from our tower and other towers in the area) at the site. Comment: Tube repeaters were not typically subject to this problem, but transmitting tube repeaters went out of style years ago.

We next checked the antenna's VSWR after the cavities. The output power is almost 100% being reflected back into the cavities. This is about a 20:1 VSWR. A 1:1 VSWR is optimal (zero power returned) and less than 1.5:1 is required for proper cavity operation. I was hoping for less than ¼ - ½ Watt reflected output. This is a no-go situation.

We then checked the lightning arrestor on the grounded skin of the building. All looks OK. It was reported that lightning was common during the last few weeks with the summer storms, but that is not the problem.

Then checked the ½" hard-line output cable from the lightning arrestor, hmmmmm – the center pin of the coaxial cable is recessed about 3/8" back from the front ring of the type N connector. It should be nearly flush with the center ring. The center pin of the coaxial cable was not connected at all to the lightning arrestor so the electrical connection was open to the antenna.

Evidently "Big Foot" was loose on the mountain during the last work party. With Big Foot walking around, the cable was stepped on and the N connector was pulled back as the refrigerator building was being painted.

We rebuilt the RF connector and re-tightened the locking ring. The VSWR is now measured at less than 1.05:1 (nearly perfect). Next we did some over the air tests with Rich, NI6H from his mobile packet radio station. All checked out OK.

Black nylon tie wraps finished the site clean up. The cables are tied up tightly so that it is obvious that this is a "DO NOT STEP" area. I will investigate making some short (6') waterproof jumper cables with male / female N fittings so that the RF cables will to lie properly on the ground. With good service loops and weatherproof sticky heat shrink tubing this problem will (should?) not happen again.

Closed up all the buildings, locked and double checked. Left the site about 2 PM.

John Kuivinen, WB6IQS
Vista, CA.

Mark KF6WTN maintains the locks to keep them in good working order for future work parties. Foreground, John WB6IQS prepares to share his Moscow Coup photo album. What a great story!

Mark KF6WTN shows the safety signage for the tower.

Mark prepares to descend into the sunken building for guide rail renovation.

Mark KF6WTN puts up the safety signs.

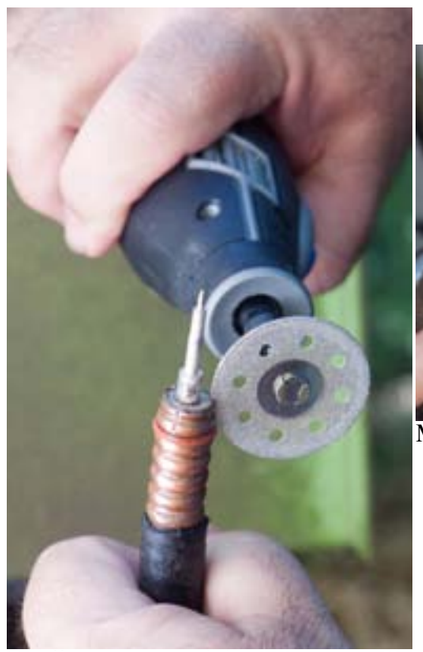
Mark and John organize for the renovation of the guide rails.

Guide rail renovation in progress.

Guide rail replacement parts.

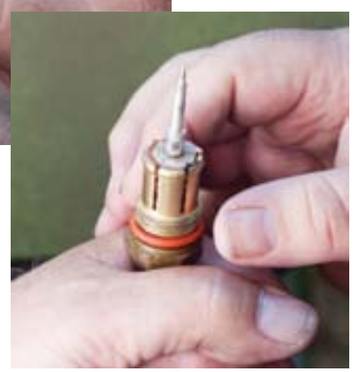
Prepared for almost anything!

Connector renovation explanation.



Small cuts to spread the connector collar.

Marking the collar for cuts.



Collar ready for refitting.

Weatherproofing!

Tightening up renovated connector.

Refitting the renovated connector.

More weatherproofing.

Michelle W5NYV did LNT duty. Four nails, trash, and a section of barbed wire were found in the driveway.

Amateur Radio at Burning Man - 10m Antenna

After the first few days at Burning Man, we had the art projects installed and under control. Our days from there were structured around scheduled music performance gigs, which left periods of time where we'd be free to hang around camp. I had installed an ISOpwr auxiliary battery isolator from West Mountain Radio and brought along a largish deep-cycle battery, to enable free use of the ham radios in the trailer without worrying about drawing down the main batteries. We had a VHF/UHF vertical mounted on a telescoping mast, but nothing for HF. In the past we had brought along a multiband vertical antenna for HF, but found the HF bands useless due to local noise. Lacking an HF antenna, I had no good way to exercise the IC-7000 in the trailer. So, I was inspired to rig up a wire antenna from junk on hand.

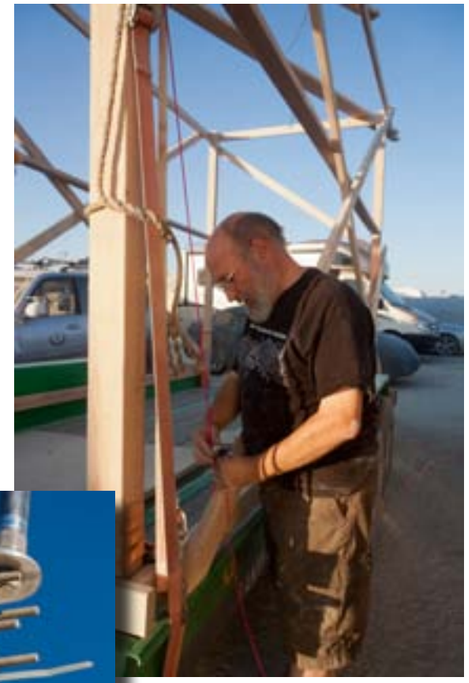
Rummaging through the storage bays of the trailer, I found some useful stuff leftover from previous antenna installations. I didn't find the big HF vertical hiding there, but I did find the length of coax and lightweight guy ropes we had used with it. Even better, I found a used SO-239 connector that I could use at the center of a dipole. Sometimes, the junk box provides exactly what you need.

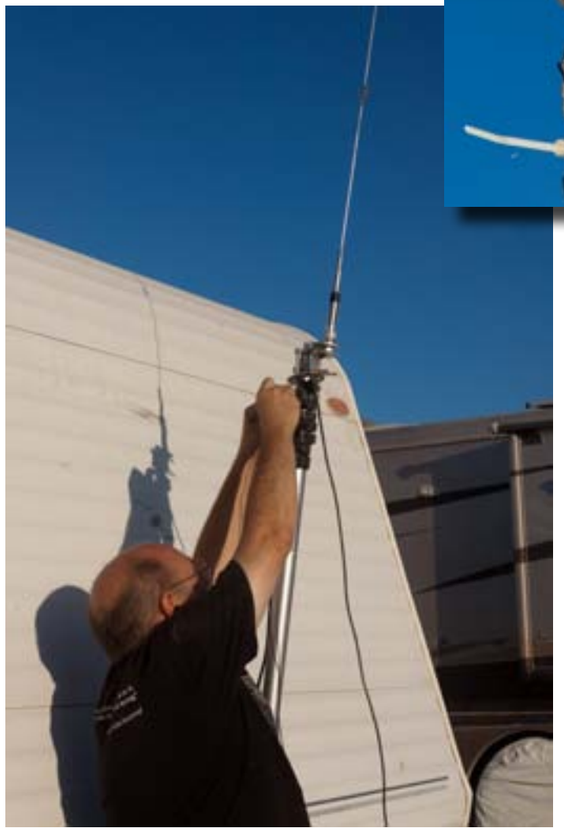
The junk box did not contain any wire, though. It's hard to make a wire antenna without wire. I had one other resource: the bins of stuff I'd brought along for repairing the art project, a MIDI-controlled pipe organ. I knew it contained soldering tools and a bunch of short lengths of hookup wire (salvaged from a scrounged length of 50-pair telephone cable). I was about resigned to soldering together lengths of hookup wire, when I stumbled upon a nice spool of insulated stranded wire I'd forgotten about. Just the thing I needed!

Dipole construction was by the book. I calculated the nominal length for a dipole resonant at 28.500 MHz using the formula we all learned for the license exam. Cut each side to length. One wire soldered to the flange, one wire soldered to the center pin. Getting fancy, I rigged up a short length of wire connected to the flange on the opposite side to serve as a strain relief for the center pin. I didn't have a balun, but then I'm not a big believer in the need for baluns with dipoles, so I wasn't worried. I tied the guy ropes to the ends of the antenna, and looked around for antenna supports. I ended up with the center connector hanging by ty-wraps from the telescoping mast. One guy rope was tied to a camp shade structure, and the other was tied to the makeshift wooden superstructure on the flatbed trailer we'd used to transport another part of the art project. It only had to last a few days, but it needed to be secure enough to withstand the high winds that are common on the playa. It was good enough. It lasted until we needed to use the flatbed trailer again.

This is where I'd like to tell you about all the amazing DX I worked with the junkbox dipole. It's a short story. 10m was dead, dead, dead, with no stations heard at all. With a tuner we could try the antenna on other bands, but only a few signals were audible. Noise levels were high, but not as high as on the vertical. Between band conditions and my compromise antenna, it was going to be tough going.

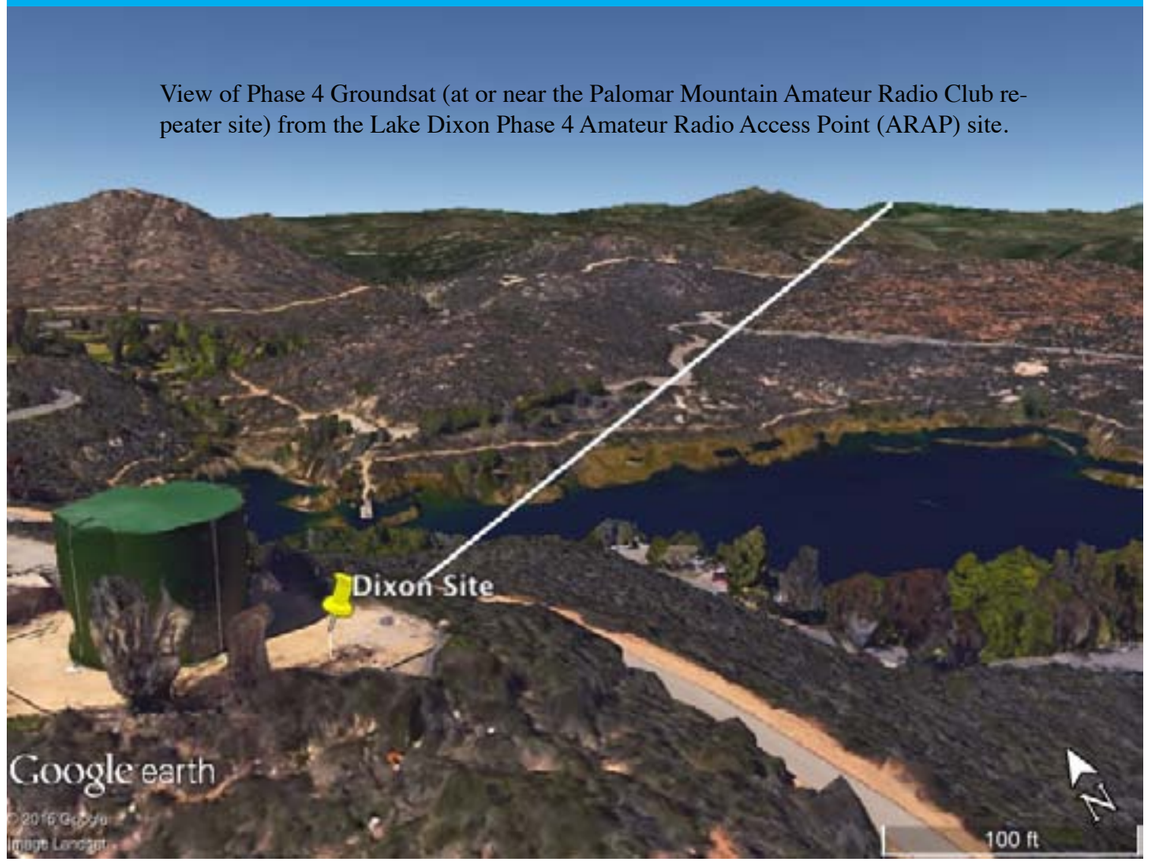
Worse, the radio was misbehaving. Whenever I tried to tune the antenna, the radio would shut off. The battery wasn't able to supply enough current, so the voltage was dropping below the radio's lower limit. This happened on both the auxiliary battery and the trailer's house battery. Apparently both batteries are at the end of their useful lives, most of which were spent sitting idle. The brownout problem disappeared when we plugged the trailer into a generator. To my surprise, the built-in house battery charger could supply plenty of current to run the transceiver at full power. I wasn't excited about running the noisy generator to get on the air, though, so that put an end to the HF experiment for this trip.





Previous page top: Wire for 10m antenna on playa surface. The soil is exremely alkaline and a very fine powdery dust.
Previous page bottom: completed 10m antenna was front and center of our art support camp. From the tent on the left, to the trailer skeleton on the right, were the Wonderlust Arcade vehicles.
This page left: detail of the 10m antenna center mast.
This page right: wire on the playa facing the street called Ersatz. It does actually look a lot like Mars!

Phase 4 Project - Site Evaluation



View of Phase 4 Groundsat (at or near the Palomar Mountain Amateur Radio Club repeater site) from the Lake Dixon Phase 4 Amateur Radio Access Point (ARAP) site.

In order to develop the hardware and software for AMSAT's Phase 4 digital satellite communications project, several terrestrial sites will be set up to simulate the system. San Diego has three proposed infrastructure sites. Two others are located in Texas and Maryland.

Components of the Phase 4 system include a satellite (the Groundsat), the gateways (Amateur Radio Access Points or ARAPs), and operators (User Terminals or UTs). The term ARAP was newly coined for our purposes. An ARAP is a gateway that allows conventional terrestrial communication links to be routed through the satellite. We will leave it open enough to include narrowband voice channels (like FM or P25) and also terrestrial data networks (like conventional wifi). Handhelds (P25, etc) that operate in support of Lake Dixon will be able to use the ARAP as an exercise and experiment. This demonstration was specifically encouraged during Bob N4HY's meeting with FEMA.

While this system is being deployed in order to more easily develop an amateur satellite service product, the development system will exist beyond the service life of the satellite, operating as a microwave amateur radio system. Mesh networking and many other services and modes are planned. Frequencies of operation include 5GHz and 10GHz. Infrastructure frequencies currently consist of links at 2.4GHz and 5GHz.

User Terminals and handhelds and any other device we can figure out how to talk to will be encouraged to join the demonstrations. We plan on deploying Phase 4 UTs with mesh networking capability built-in. The Palomar Amateur Radio Club has been asked to promote this aspect of the demonstration. Phil KA9Q has agreed to chair a PARC technical committee in order to coordinate and

promote mesh networking. Our intent is to be compatible with terrestrial mesh networks such as HSMM, BBHN, AREDN, and others.

The Groundsat will be located on Palomar Mountain. PARC has been asked to host the hardware, donated by Ettus Research and Virginia Tech. The Groundsat simulates a satellite. ARAPs are either fixed or mobile aggregators. Operaters with radios insufficiently strong enough to close a satellite link communicate with the ARAP, and the ARAP communicates with the satellite. UTs are radios that are satellite capable, and communicate either with an ARAP or directly with the Groundsat.

The second proposed site for Phase 4 infrastructure in San Diego County is at Lake Dixon. This is proposed to be an ARAP site.

The third proposed site for Phase 4 infrastructure is a mobile unit that will be based from Phil KA9Q's QTH. Equipment purchased will be donated to PARC.

Preliminary approval for the Groundsat has been granted by PARC. Discussions are ongoing with Dixon Lake Ranger Station for AC power for the ARAP.

Site evaluation for Lake Dixon and Palomar revealed a line of sight path (see image on previous page). Radiomobile link evaluations were carried out at Virginia Tech.

A visual evaluation was made at KA9Q's QTH. Several other sites around San Diego are being considered for additional hardware, but the minimum configuration is Palomar and one other ARAP site. With at least three sites in negotiations, Phase 4 is in great shape for hardware and software development!

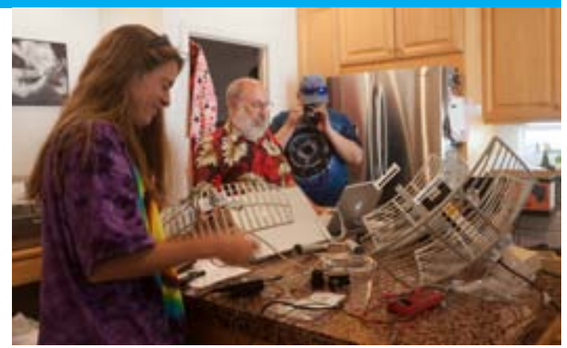
The water tank already serves as a cell tower.

This pole at Lake Dixon was considered as a possible place for mounting infrastructure hardware.

The view towards Palomar Mountain over Lake Dixon.

Phase 4 Project - Backhaul Configuration

Unboxing! Thank you Zach at Virginia Tech!



Kathy KA6OYD and Paul KB5MU and Bob N4HY

Sorting the equipment at Lake Dixon.

Kathy, Paul and Phil KA9Q

Some good expressions from the sorting and planning session.

Join us! Volunteers welcome.
Must be US citizen due to ITAR.
Contact w5nyv@yahoo.com.

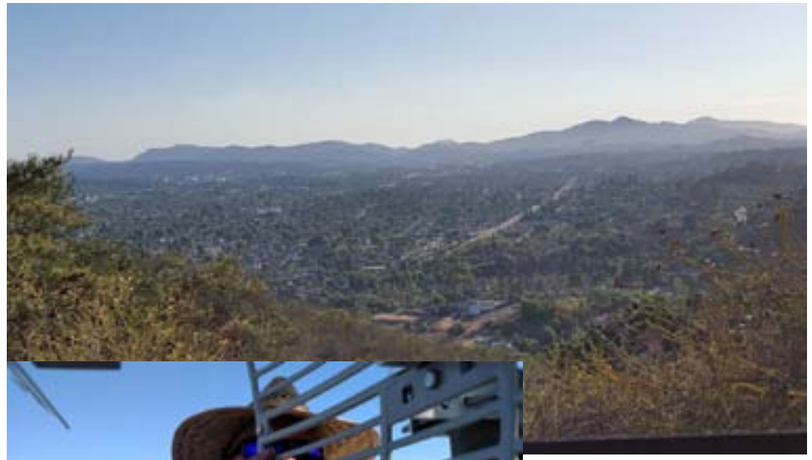
Paul, Bob and Phil continue the configuration at Paul's QTH. This was a successful and enjoyable evening spent configuring the development system, eating out at a local restaurant, and telling lots of tall tales!

Kathy and Paul notice one bullet won't reset.

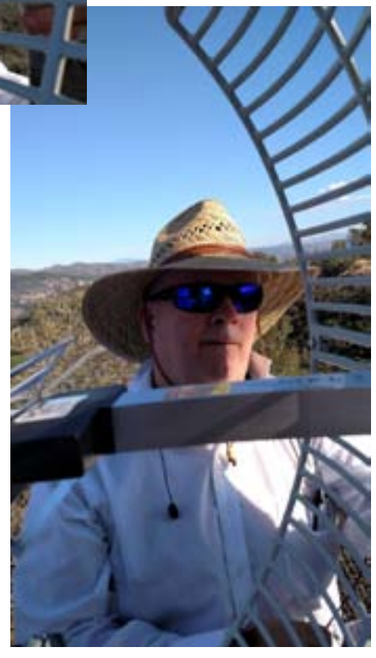
With a special tool (golden paper clip), the reset function was finally activated and the last bullet could be updated and configured.

Phil KA9Q reviews the troops. All bullets communicated successfully at the configuration party.

Phase 4 Project - Dixon Equipment Installation

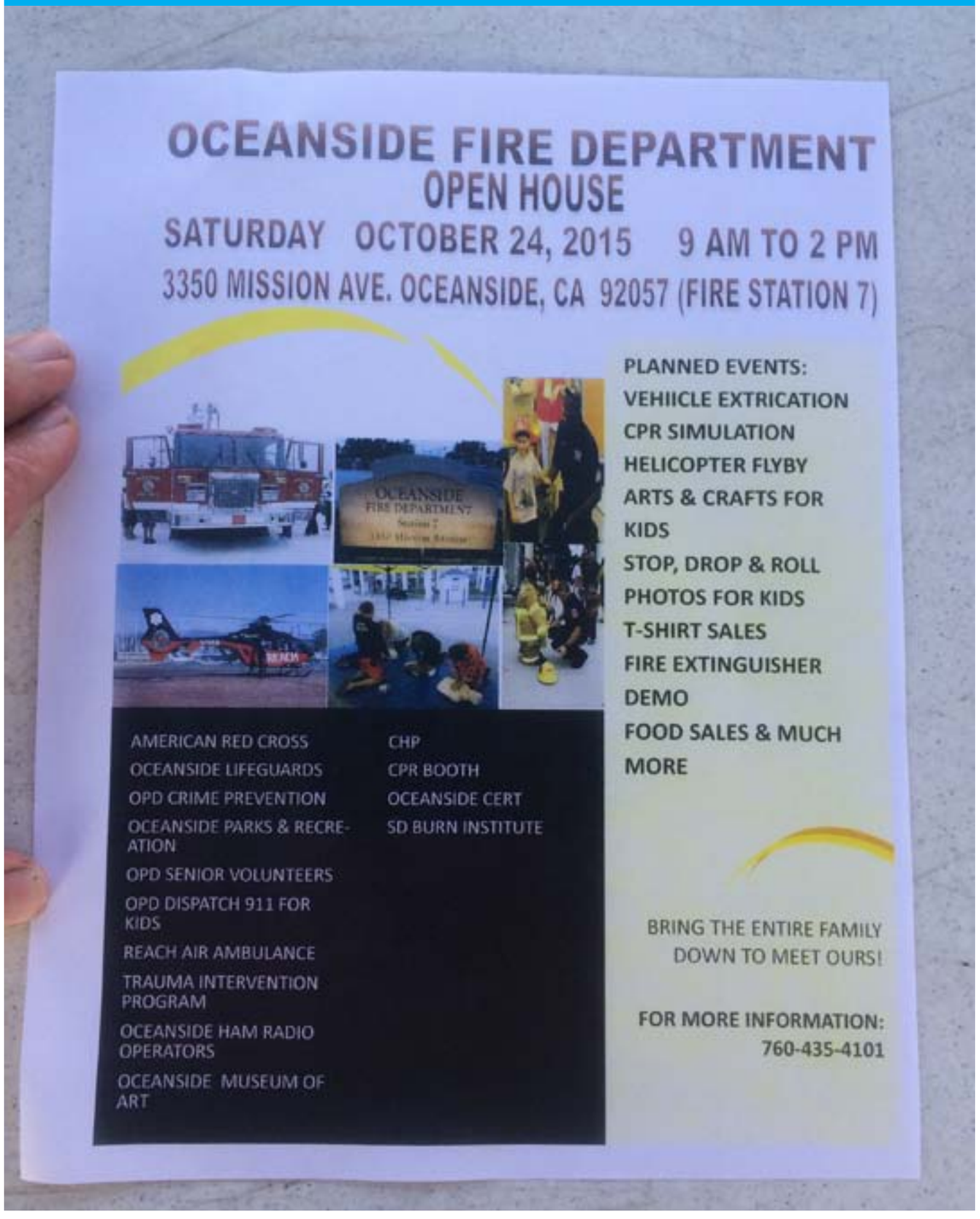


Bob N4HY installs one of the two dishes that the backhaul will use at Lake Dixon.



Solar power is being investigated for the Lake Dixon ARAP.

Upcoming PARC Demonstration! 24 October



Lunch Bunch 25 September 2015 at Callahan's

The Ham Radio Lunch Bunch meets Fridays for lunch and socializing at any one of a number of restaurants on a rotating schedule.
The Lunch Bunch signup is http://w0ni.com

Reminders are sent out on Wednesdays.
All are welcome for food and fun!

Some of the restaurants on the schedule are Fuddruckers, UTC Food Court, Spices Thai, Savory Buffet, Denny's, Callahan's Pub and Grill, and Phil's BBQ.

SCOPE
P.O. Box 73
Vista, CA 92085-0073

PERIODICALS

Return service requested

Scope Volume #47 Issue #10 (USPS #076530) is published monthly by the Palomar Amateur Radio Club 1651 Mesa Verde Drive, Vista, CA 92084.
POSTMASTER: Send address changes to SCOPE, P.O. Box 73, Vista, CA 92085. Periodicals postage paid at Vista, CA 92084 and at additional mailing offices. Dues are $20 per year or $35 per year for a family. Dues include a subscription to Scope.
You can join or renew your membership, find a repeater listing, find contact information for the board all on the club's web site http://www.palomararc.org

Editor: Michelle Thompson W5NYV
Submissions: scope@palomararc.org
Questions? Ideas? Comments? W6NWG@amsat.org

Featured Program:

On 7 October 2015, Palomar Amateur Radio Club will present our annual auction. See page 21 for details. We look forward to seeing you at the Carlsbad Safety Center, 2560 Orion Way, Carlsbad, CA.

Sign up for the PARC Email Lists:

http://www.palomararc.org/mailman/listinfo