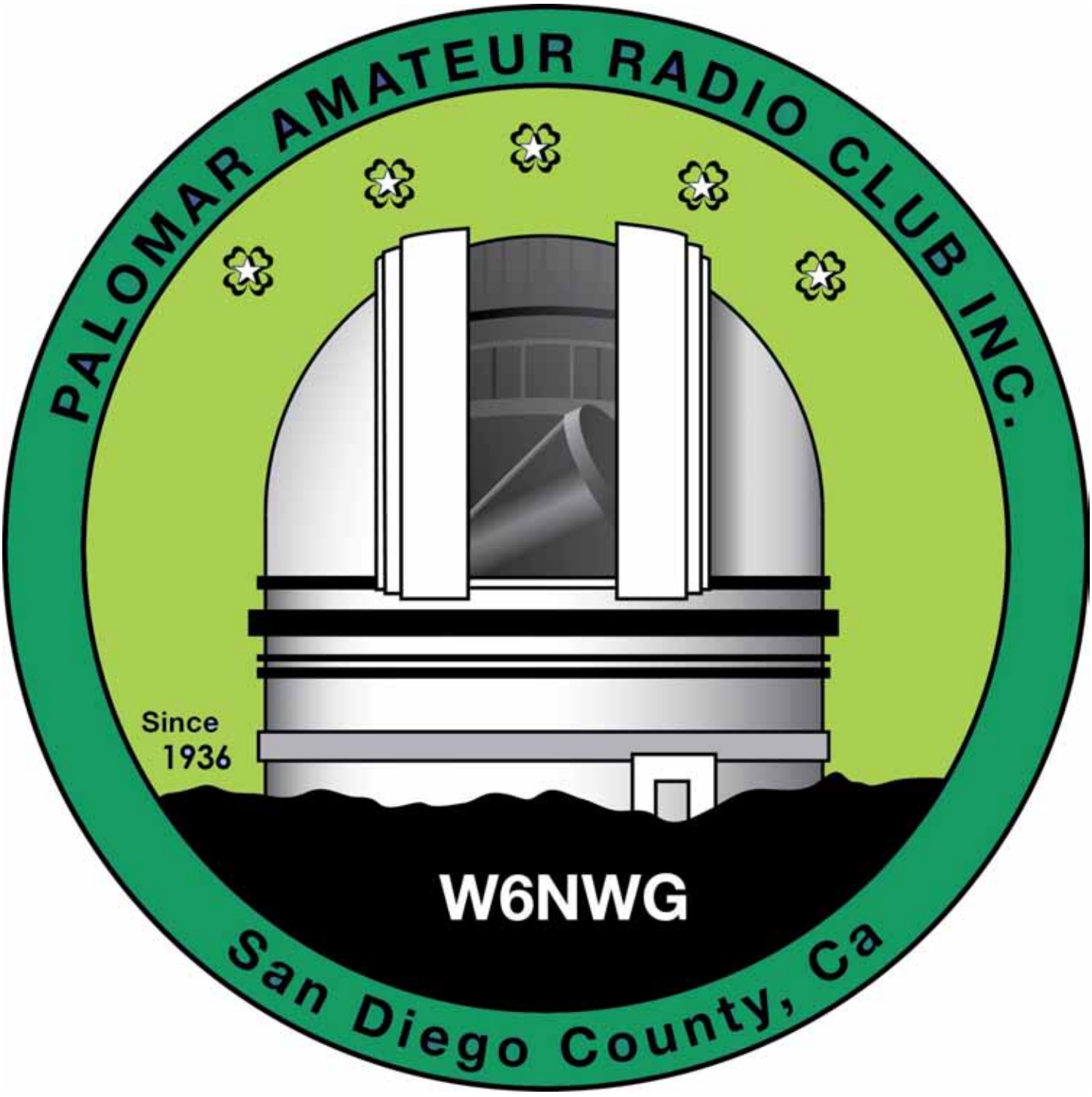

PALOMAR AMATEUR RADIO CLUB INC.
Since
1936
W6NWG
San Diego County, Ca

Club
Meeting 7:30pm
2 March 2016

Carlsbad Safety Center,
2560 Orion Way, Carlsbad

Program is about AREDN by
Andre Hansen K6AH.

Visalia International DX
Convention

15-16 April 2016

see page 11 for details

PARC
Board of
Directors Meeting
7pm
9 March 2016

14322 Pomerado Road,
Poway, CA 92064

Many of us enjoy creating phonetics to help others remember our call signs, such as my friend Wayne KA7WBE, a professional radio technician, who used the phrase: Wet Behind the Ears. These things stick with us.

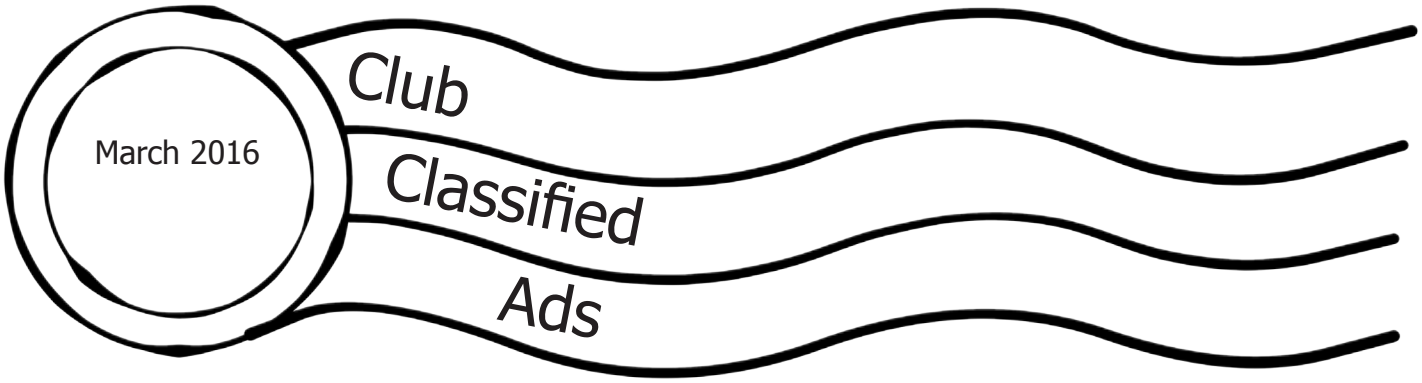
They do create problems, however, when we are spelling out words or names in our radio transmissions. In the high speed of emergency communications, for example, when we use the word "sugar" to represent the "s," those copying us may have a slight hesitation before they realize that that the sh- really belongs to a word that starts with "s," and in that fraction of a second, the next letter or letters can fly by unheard. Even an obvious word like "umbrella" instead of "uniform" can cause a slight pause for recognition.

When we use standard ITU (or NATO) phonetics, however, we and those copying us should get so accustomed to using and hearing those same words over and over that our minds can recognize them immediately, and we can then write whole words or names automatically, keeping our thinking open for content. Of course, Perfect Practice Makes Perfect, so the more we use these phonetics, the more comfortable we become with them and the better and faster our communications can be.

by John AC7GK

AUCTION IPAD HELP NEEDED

If anyone knows the person who donated the ipad to last October's auction, please have them contact KK6EED@amsat.org. We cannot reset the defaults without your help!



This is NOT AN AD!

But it could be!

FOR SALE!

SignaLink USB Sound Card Interface & Accessories

- SignaLink USB p/n SLUSB6PM
- Plug & Play Jumper Module p/n SLMODHT
- Plug & Play Jumper Module p/n SLMOD6PM
- Extra Radio Cable p/n SLCABHTY

All items brand new, all for $75.

de Bill KK6LWE@arrl.net

Advertisements are free for members

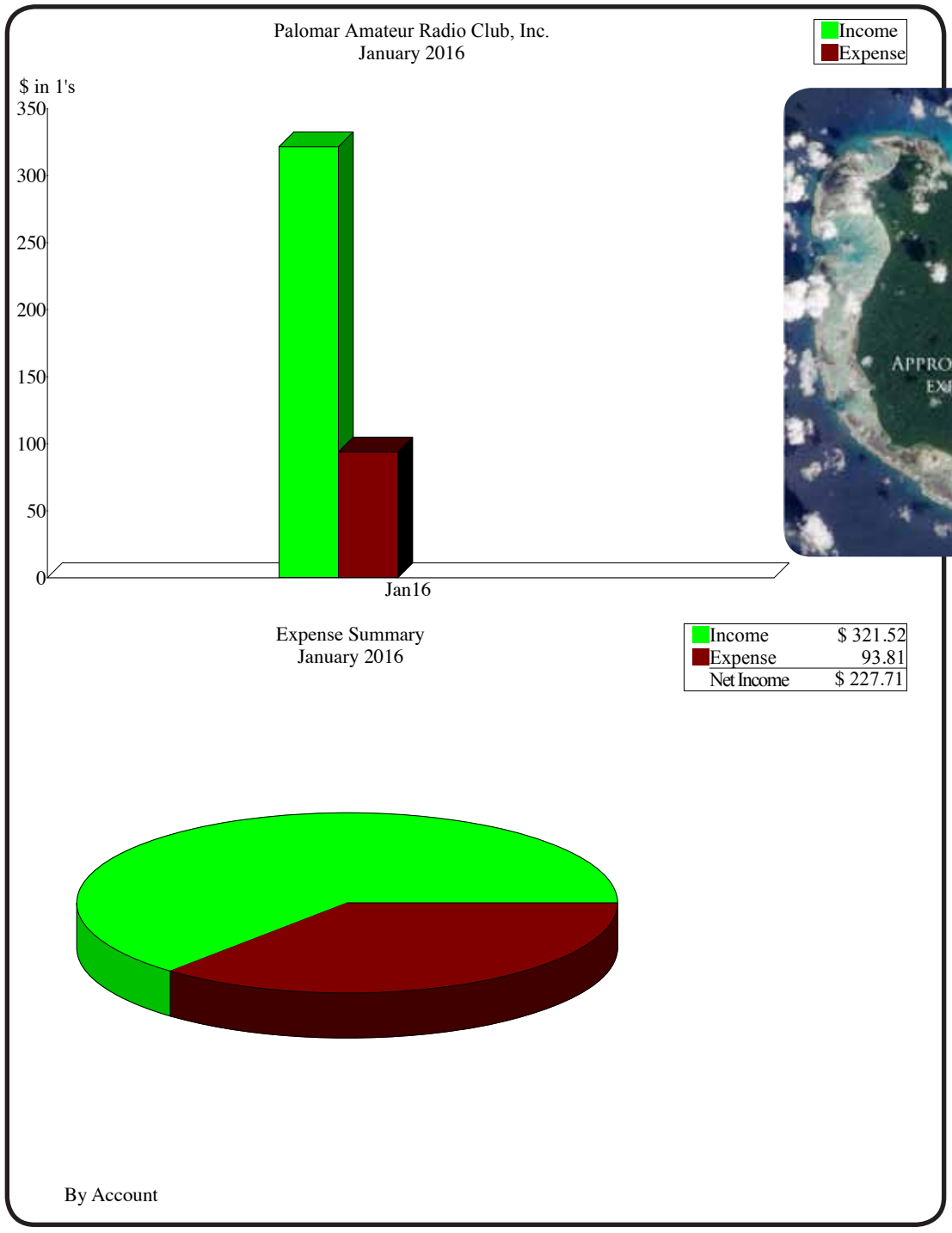
Have items that need to find a new home? Advertise here! Send your ads to scope@palomararc.org

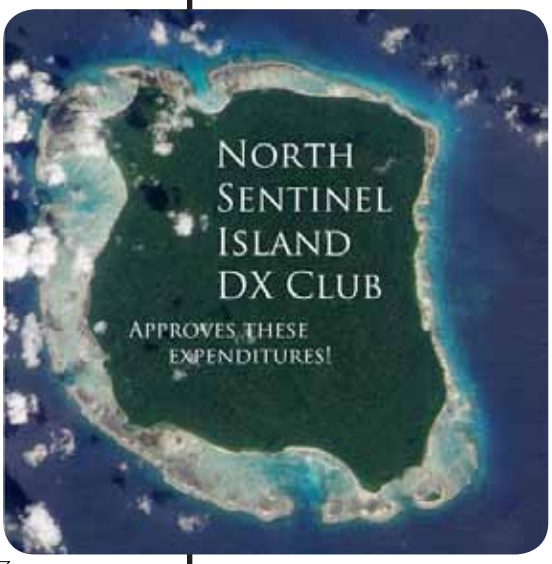
Club Members ONLY!
PARC has a tube bank that includes many 6 & 12 volt receiving tubes (and some transmitting types) for use by club members to repair their own personal equipment. Not for commercial use or resale. If we have your requests, we will pre-check the tubes and deliver them to you at the next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

Contact John WB6IQS WB6IQS@att.net

22 February 2016

Club Financial Update





Expense Summary
January 2016

Income	$ 321.52
Expense	93.81
Net Income	$ 227.71

By Account

Committee Chairs and Board Members Contact Info

February 2016

Current Board of Directors

President	Charlie Ristorcelli NN3V	(619) 368-7617
Vice President	Joe Peterson K6JPE	(619) 630-8283
Treasurer	Tom Ellett W0NI	(858) 546-1148
Secretary	Sandy Pratt KK6EED	(858) 748-2611
Director #1	Kevin Walsh KK6FRK	(858)722-5069 (text welcome)
Director #2	John Walker AC7GK	(949) 212-5533
Membership Chair	Glen Christensen KJ6ZQH	(858) 735-1144
Repeater Technical Chair	Mark Raptis KF6WTN	(760) 672-0223
Scope Editor	Michelle Thompson W5NYV	(858) 229-3399 (text welcome)

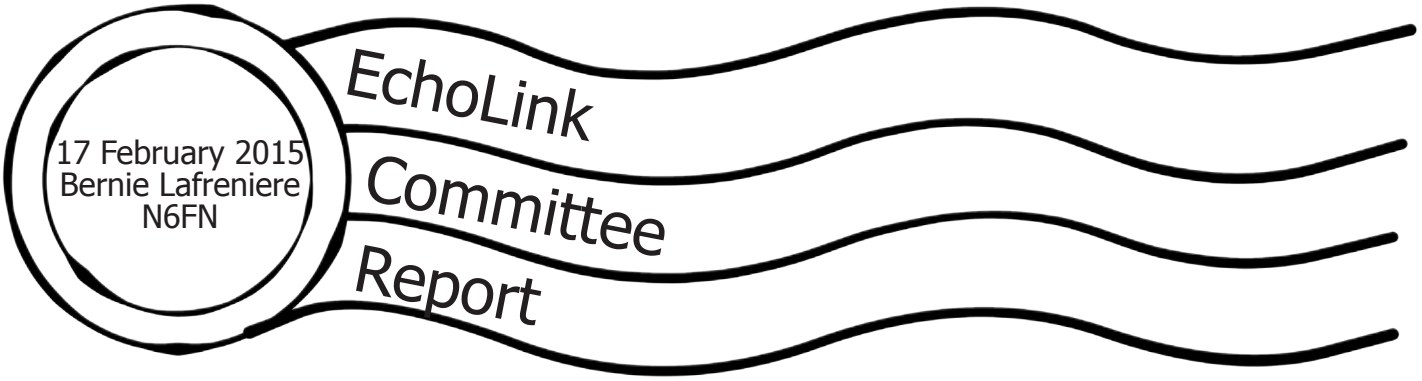
Not on the Board

Repeater Site Chair	Mark Raptis KF6WTN (acting)	(760) 672-0223

The board members might have callsign@amsat.org mail aliases.

Committee Chairs

EchoLink	Bernie Lafreniere N6FN	N6FN@niftyaccessories.com
mesh networking	Phil Karn KA9Q	karn@ka9q.net
Operating Day	Tom Martin K6RCW	k6rcw@amsat.org
SANDARC Representative	John Walker AC7GK	ac7gkjohn@gmail.com
SANDARC Representative	Paul Williamson KB5MU	kb5mu@amsat.org
SANDARC Alternate	Michelle Thompson W5NYV	w5nyv@amsat.org
SD Microwave Group Liaison	Kerry Banke N6IZW	kbanke@sbcglobal.net



Because of a lack of control flexibility of the Yaesu DR1X repeaters, configuring the EchoLink node for operation on our new DR-1X 447.000 repeater requires bypassing the internal controller built into the DR-1X and controlling the repeater's operation using an external controller.

The Yaesu repeaters were designed to be compatible with Yaesu's AMS (Automatic Mode Select) concept, wherein a single repeater can automatically switch between standard (legacy) analog FM operation and Yaesu's C4FM System Fusion digital operation. Consequently the Yaesu engineers did not design in the "normally" encountered features found in a general purpose repeater controller. The use of an external commercially available general purpose controller will be able to rectify that situation, allowing us full control of the repeaters.

Two commercial controllers that are known to have worked with the DR-1X have been evaluated and a selection of one of them has been made. We are in the process of ordering one of the controllers for configuration and testing with the Palomar repeaters.

Beyond updating our Yaesu DR-1X repeaters with new external controllers, the investigation of the controller will attempt to configure and use the same controller to replace the controllers on our set of older repeaters. The objective is to be able to control our entire set of repeaters using the same method of control.

The first task will be to configure the new controller to be able to operate all of our Yaesu DR-1X repeaters on Palomar Mountain. As part of that, EchoLink operation will be restored to the 447 machine. After that has been accomplished, the task of converting our older repeaters to operate with the new controllers will be undertaken.

President's Corner

March 2016

By the time you read this, the Yuma hamfest will be a dimming memory. But what a pleasant memory it is. Truly a nice hamfest. The Yuma hams continue making it better and better. I saw many PARC club members in attendance, and some were selling excellent "toys" in the tailgate area.

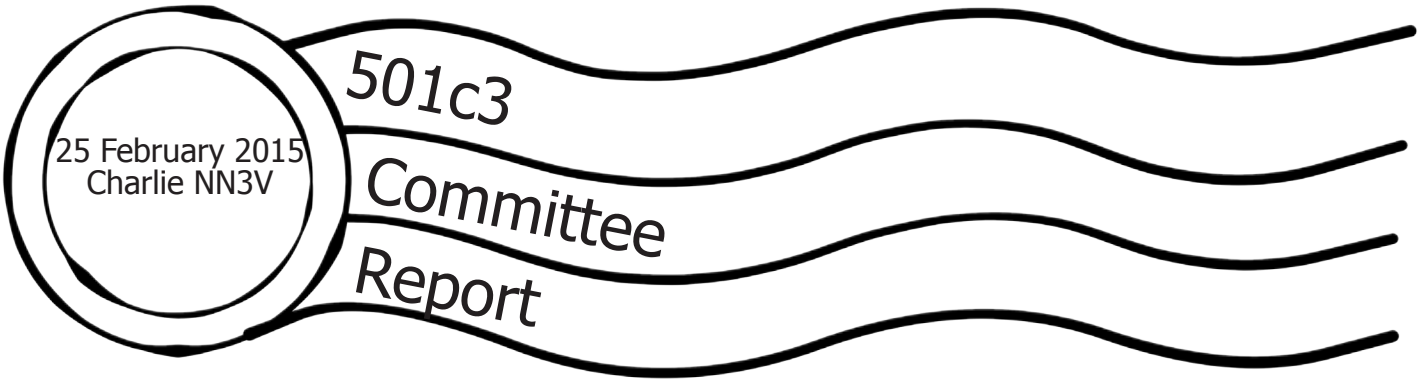
The icing on the cake was to see two PARC members win some of the grand prizes. KJ6ZQH (Glen) our membership chair won a very nice Kenwood dual band mobile that is APRS ready. And KD6TUJ (Dennis) walked off with another fine dual band mobile, in this case a Yaesu FT-7900. In Glen's case, not too shabby a showing for the first time he's ever attended a hamfest!

Our friend N6KI (Dennis) presented a wonderful program about Viet Nam era MARS operations and the phone patches he ran for many, many Viet Nam service members. The hamfest audience gave the presentation a standing ovation. Indeed, Dennis' program is certainly worth seeing if you have a chance.

N6AA (Richard Norton), the ARRL Southwestern Division Director hosted the ARRL forum. As the hamfest was also the Southwest Area ARRL convention, the forum is a standard feature at all ARRL events. It is an opportunity for ARRL Officers to interact with the local ARRL membership and answer questions about ham radio policy, as well as become aware of local ham radio issues. The hottest issue discussed was the status of the Ham Radio Parity Act, the legislation moving through congress that will require HOA organizations to allow ham operators living in the HOA to install ham radio antennas.

You can learn all the details about the Ham Radio Parity Act by surfing your browser to http://www.arrl.org/amateur-radio-parity-act.

You owe it to your fellow hams and your very own interest to support efforts to pass the legislation by contacting your elected representatives. The ARRL article at the link will give you all the details needed to do so, and will even link you to web sources that will guide you in the contact procedures.



PARC was designated a non-profit public benefit charity in July 2015. Since then the club's treasurer has been empowered to offer tax donation receipts, should they ask for any, to any donor of material or funds to the Club. Note that the tax benefit to the donor only applies if the donor is eligible to itemize deductions on their annual tax return. That depends on the donor's annual income and tax situation. If you want to know if you qualify, consult your CPA, or read the tax rules very closely. PARC also registered with Amazon to receive donations from any purchase ordered on www.smile.amazon.com

This has been commented upon in other places in Scope. It would be nice if you supported PARC by making your Amazon purchases by ordering at that website. When you place your order, you will be offered an opportunity to pick the non-profit to which Amazon's donation will be made. Pick Palomar Amateur Radio Club. It has absolutely NO IMPACT on your purchase price. So if you are buying something on Amazon, why not ask Amazon to make a donation to PARC?

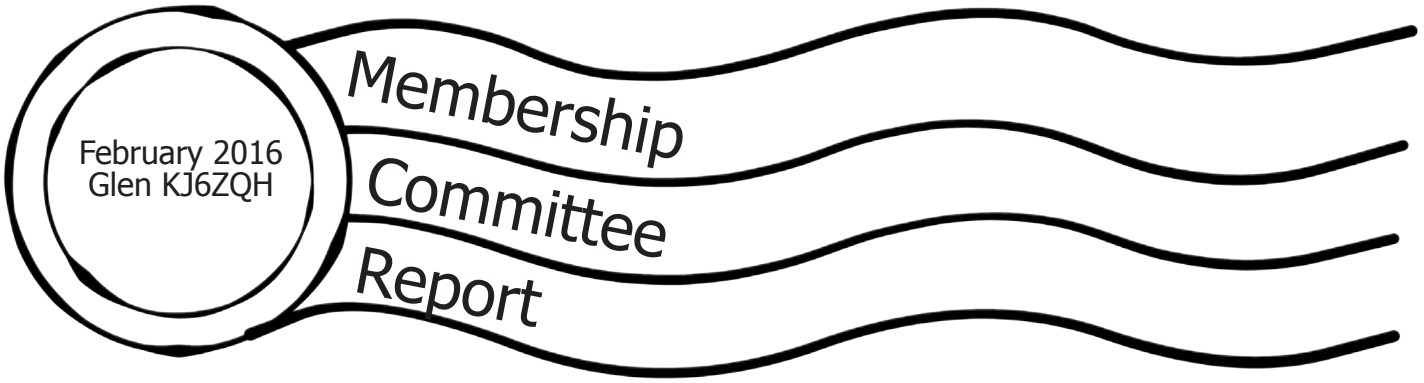
So how has the club faired in the non-profit world? Initially several club members donated funds to help the club transition to the electronic processing of Scope. The donated funds paid for unexpected processing expenses. Funds were also donated to allow the technical chair to implement minor hardware fixes to the Club's Palomar Mountain infrastructure.

This year the non-profit status is allowing the Board of Directors to plan significant improvements in our infrastructure. Courtesy of a Club donor, we are now in the midst of acquiring and planning the installation of brand new, commercially-procured repeater cavities for our 6-meter repeater. Along with that, the entire repeater will be upgraded. The donation was for funds in excess of $3000.00

Similarly, donors have contributed funds to permit the Club to buy brand new controllers that will allow remote control of all the repeaters on Palomar Mountain. This too is a significant donation. When fully implemented the repeaters should have the courtesy tone restored, as Yaesu has acknowledged such courtesy tone cannot be implemented in the AMS or analog mode of operation as designed by Yaesu. The new controllers will assist in restoring the Palomar Mountain Echolink node we had on the 447 machine.

Getting all this new hardware implies that there will be a lot of interesting and rewarding "hand on work" opportunities to assist in getting all things set up.

If you are willing to help, please contact KF6WTN (Mark) and offer your help. You may do so by sending email to board@palomararc.org



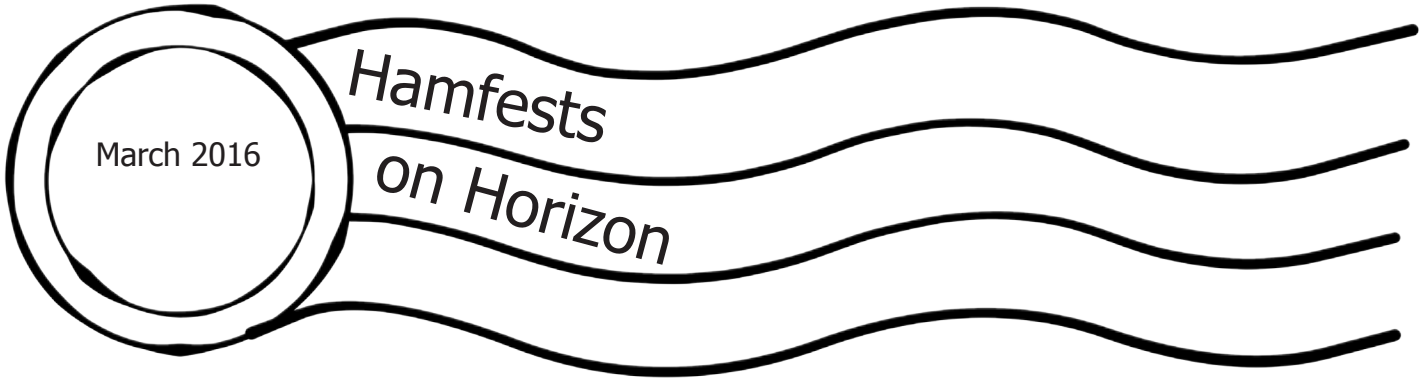
From the Membership Table

You can check the status of your membership 24/7. Go to the club's website and navigate to Join and click on "here" at the top of the page. Enter your call sign into the box and click the "Look up my membership status now" button.

To renew your membership or extend your membership, fill in the form on the Join page. Make sure you select the correct value from each of the drop-down menus (Type of Membership, How many years, I'm an ARRL Member, Newsletter option and License Class).

If you want to receive an email when your membership is coming due for renewal, please make sure that I have a valid email address for you. To do that, please send an email to Membership@palomararc.org.

73,
Glen KJ6ZQH, Membership Chair



The time is near for you to be thinking about going to a hamfest. And there are some on the horizon that are really very good.

The **Palm Springs Hamfest** will take place on Saturday, March 12. See

http://palmspringshamfest.com

The **Visalia International DX Convention.** If you have any interest in HF communications, or if you are an avid DX chaser, this is a top notch event, and easily reachable from San Diego. There are many opportunities to ride share, and if you are interested, come up on the repeaters and mention you are looking for a ride. The hamfest / convention takes place at the Visalia California Convention Center on April 15 – 16. There you can enjoy all the traditional fun of a hamfest, and you will be treated to exceptional presentations by some of the world's top DXers. You can find out all about this at:

http://dxconvention.org/

The **Dayton Hamvention**. Start planning now! If you are a ham and have not been to Dayton at least once in a lifetime, then you are not yet "a real ham! Just kidding of course, but there is no question that Dayton is the largest amateur radio event in the world. Getting to and from Dayton is relatively inexpensive as Southwest and other bargain airlines offer excellent fares. And hotel accommodations in the vicinity of Hara Arena are very reasonable. Ignore the rumors you've heard about there being no Hamvention because Hara arena is falling down. Not true. It is in need of extensive renovation, but repairs have begun. And if you are looking for something about ham radio and cannot find it at Dayton, then it has not been invented or created yet! Dayton takes place at Hara Arena, Dayton, Ohio, the weekend after Mother's Day: May 20 – 22, and you can read all about it at:

http://hamvention.org/

Love hamfests? Looking for one a little closer to home?

The Next **San Diego Ham Fest** will be in October 2016 Exact date: TBA
Location: Lakeside Rodeo Grounds located at 12584 Mapleview Street in the town of Lakeside

http://www.lakesidearc.org/sdhamfest/sdhamfest.php

Registration Required – Limited Seats

Oceanside CERT ACADEMY

Starting March 3, 2016

Applications Due March 1, 2016

SCHEDULE:	**March 3, 5, 10, 12**
TOPICS:	**Disaster Preparedness, Fire Safety, CERT Organization, Search and Rescue, Disaster Medical Operations, Disaster Psychology, Terrorism and CERT, A Course Review and Disaster Drill**
TIME:	Thursdays – 6:00 to 10:00 pm Saturdays – 8:00 am to 5:00 pm
LOCATION:	Oceanside Fire Training Facility 110 Jones Rd, Oceanside, CA 92054

Participants are encouraged to bring a brown bag lunch each day. Coffee and water will be supplied.

HOW TO APPLY: Interested participants must complete a CERT Application and submit it by March 1, 2016 to Oceanside CERT, c/o the Oceanside Fire Department, 300 North Coast Hwy, Oceanside, CA 92054. Applications are available at www.oceansidecert.org.

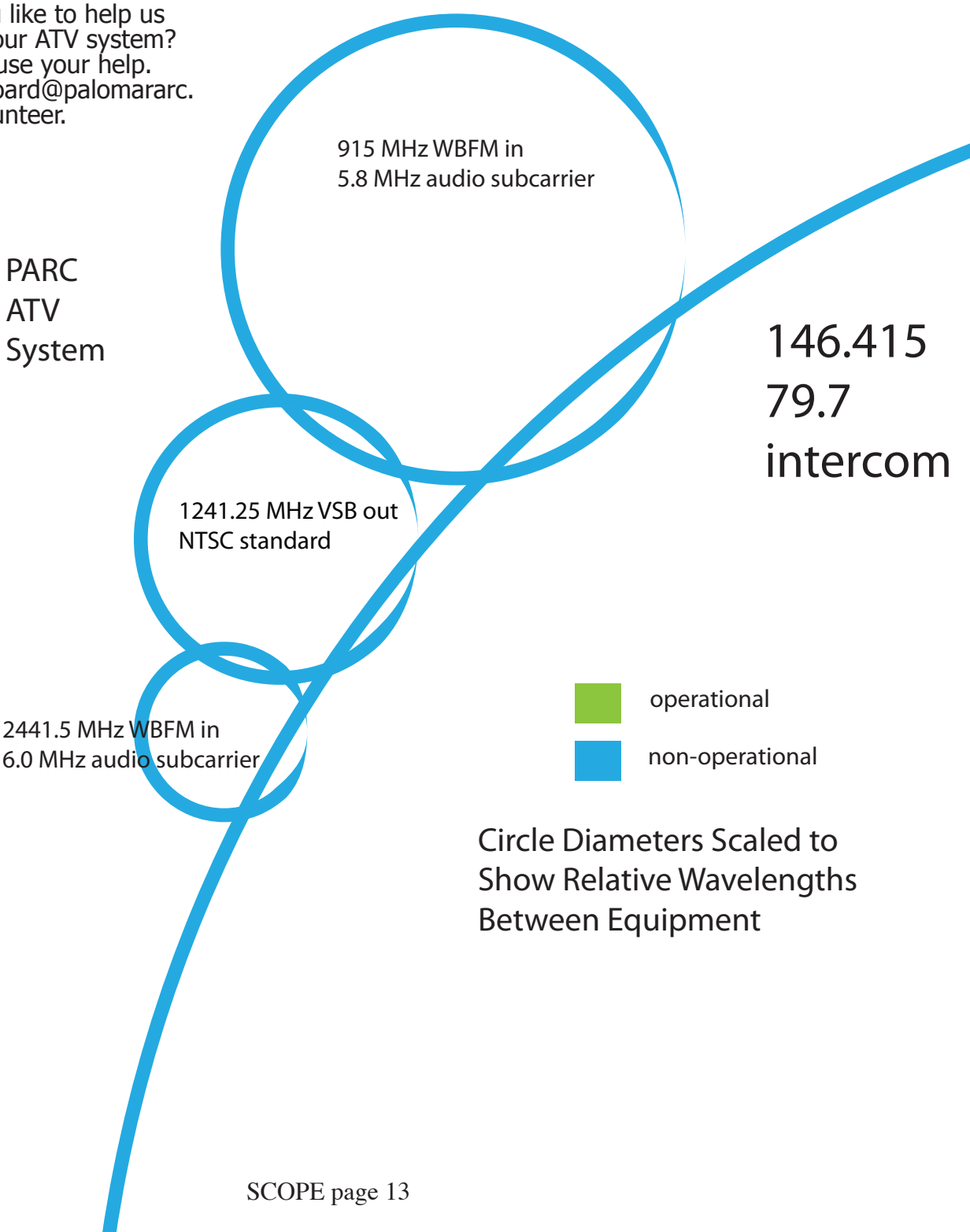
The CERT Academy is designed to prepare you to help yourself and to help others in the event of a catastrophic disaster. This training covers basic skills that are important to know in a disaster when emergency services may not be available.

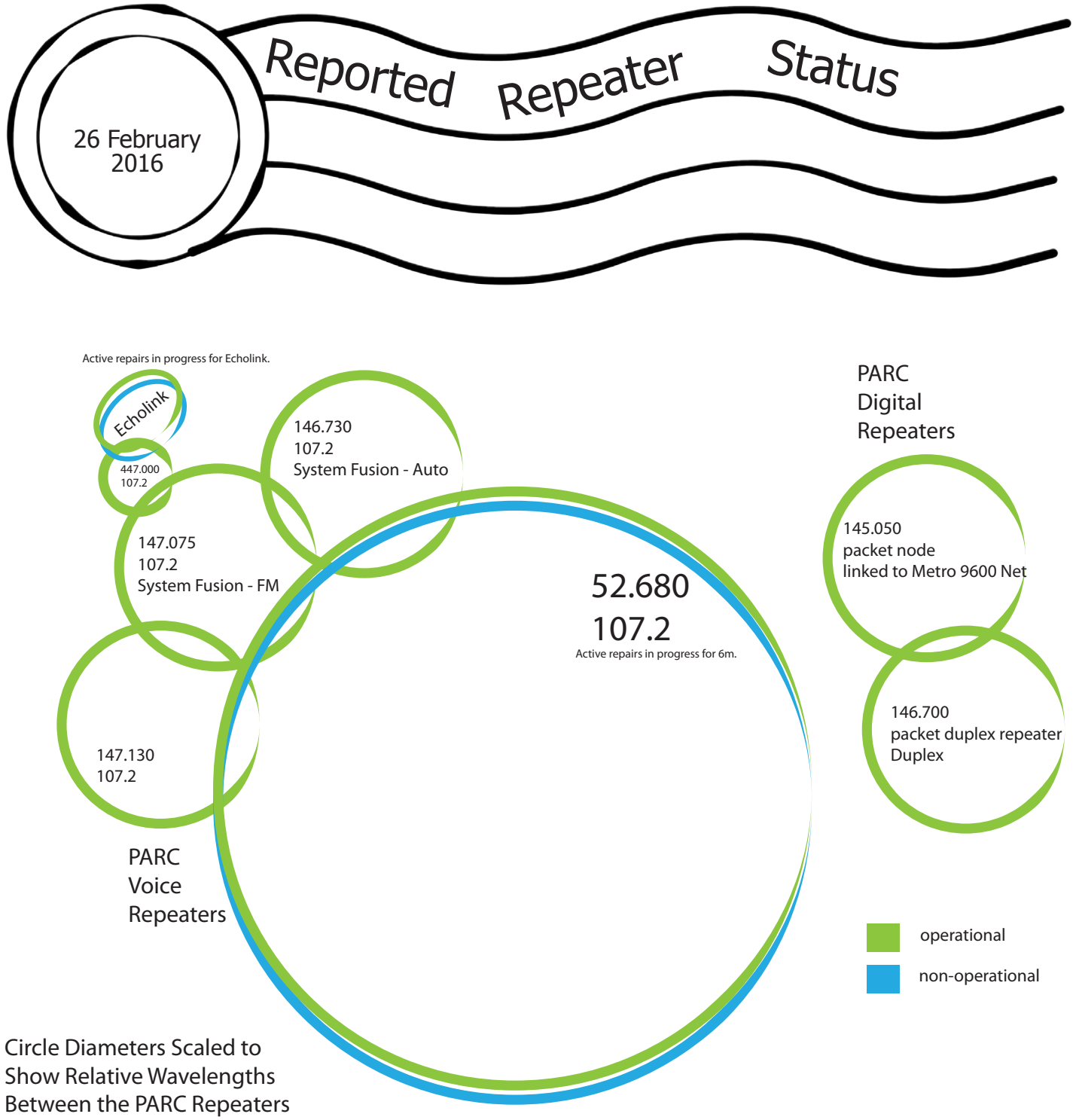
For more information on Registration and Oceanside CERT please visit www.oceansidecert.org

Reported ATV Status

26 February 2016

Would you like to help us revitalize our ATV system? We could use your help. Contact board@palomararc.org to volunteer.





See Bernie Lafreniere N6FN's report on page 7 for the latest news about EchoLink repairs.

Substantial 6m repeater repair progress has been made by John W6JBR and others. See 501c3 committee report on page 9.

February 2016

February Membership Meeting Report

Photos by Sandy Pratt KK6EED

Watch this presentation at our Palomar Amateur Radio Club YouTube Channel:

https://www.youtube.com/PalomarArc

Direct Link:

https://www.youtube.com/watch?v=ZfW9rwcnn5M

Amazon Shopping for PARC

Shop on www.smile.amazon.com
Same thing as shopping on Amazon
BUT! when you shop at www.smile.amazon.com
If you designate Palomar Amateur Radio Club
As your charity of choice, Amazon will
Donate to PARC!

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

{special} THANKS to our sponsors

There is good news about our club's non-profit status. As mentioned in December, PARC is now a tax exempt non-profit public corporation. if you choose to donate money or equipment to PARC, and if you itemize deductions, you can take a tax exemption for the value of the donation.

BUT There is even an easy way to donate to PARC! Do you shop online at Amazon?

PARC is now registered with smile.Amazon.com as a not-for-profit public corporation. If you so choose, any purchase you make on Amazon can be identified as a purchase for which you desire that Amazon donate funds to PARC!

Here is how it works.

If you wish to designate that some funds of your Amazon purchases be donated to PARC, go to www.smile.amazon.com and log on to make your regular purchases just as you always do. After logging in, you proceed to order your purchase as usual, and in the checkout procedure you are offered an opportunity to designate a portion of the purchase to be distributed by Amazon to any of thousands of charities. There we ask that you select "Palomar Amateur Radio Club" as the non-profit to which the funds will be donated by Amazon.

This will have absolutely NO EFFECT on the regular purchase price of your item.

What happens is that without any further action on your part, Amazon will forward to PARC's bank account 0.5% of the purchase price of what you bought.

You can learn all about this further by visiting the following link:
https://smile.amazon.com/ch/95-3737299

Amazon is aware of one problem with this initiative. **The Amazon smartphone shopping app DOES NOT work for charity designations. You must use the web browser.**

Your PARC Board of Directors hopes you will consider donating to PARC as you shop on Amazon. The Board of Directors is evaluating a series of projects to update the Club's infrastructure, to bring remote capability to PARC members, to upgrade our FD equipment, and to update the technologies we have available throughout our repeaters. Some of these projects are the result of your response to questionnaires, or suggestions you forwarded to the board for consideration. All these potential projects will be evaluated and announced to you so you can give us feedback about the project's desirability. To carry the projects to completion will require that club member volunteers get hands-on experience in the project. This too will be an opportunity to follow the requests expressed by members, and also an opportunity to elmer recent licensees in all aspects of ham radio.

You asked that the Club be revitalized in this manner, and here are the beginnings of the effort. So please remember, when you shop on Amazon, donate to your club! But they will all involve material purchases for which the Club will be using funds that are donated for the project accomplishment.

We hope you will be generous in donating to PARC through Amazon purchases since the donation has zero impact on what you buy.

Greetings from Skiathos, Greece. (Zulu + 3 Hrs)

I know this is not what many of you think of this as a traditional DXpedition but it has taken me similar costs and planning to try to pull this off.

XYL and I are on board the Sea Dream 1 a small cruising Yacht in the Agean Sea heading towards Istanbul.

Tomorrow September 08, we will be sailing by Mt Athos SV/A a particularly rare DX location because the only licensed ham is Monk Apollo who is limited on the number of days a year he can speak. Mt Athos is a celibate religious principality where women are not allowed and landing is only permitted for men with permits reserved for adherents to the local religious practice.

Needless to say I do not qualify for a permit and Monk Apollo jealously guards his ham exclusivity so they never authorize third party ham operations To add to the difficulty the yacht captain refuses to land on Mt Athos because he would be fined and lose his transit permits.

However if you are willing to throw enough money at a problem there is invariably a solution.

I have engaged a Zodiac (large rubber boat) to rendezvous with the yacht to take me and my equipment (Ipad, Bluetooth headset, 4G Wifi Hotspot, MacBook Air, external Wifi Hotspot antenna) as close as possible to Mt Athos.

It will be remote country #26 for me via my Flex SDR radios.

I hope to actually put a foot or two onshore while making a QSO albeit everyone locally seems to be rather afraid of the religious authorities. However a few extra €$ seems to have mitigated those fears somewhat.

The Zodiac Rendezvous is supposed to be at 0500Z 09/08/15. I should be ashore around 0515 bit could be delayed by weather for hopefully 5-15 minutes or as long as the Zodiac owners are comfortable that they won't be hit with a big fines (I get to pay any fines)

I plan to use 14.195 BUT the the Over the Horizon Radar blazing away, I may move up 10-20Khz.

I will be remoting to my station KY6LA in La Jolla, CA somewhere around 0500-1000z...to my Flex 6700. I will be using one or two of several different Remote Apps....Parallels Access for IPad, K6TU remote for iPad, and Don Agro's MacBook App for Flex. .. Amazing how many remote options there are for the Flex now without the need for any extra equipment at home.

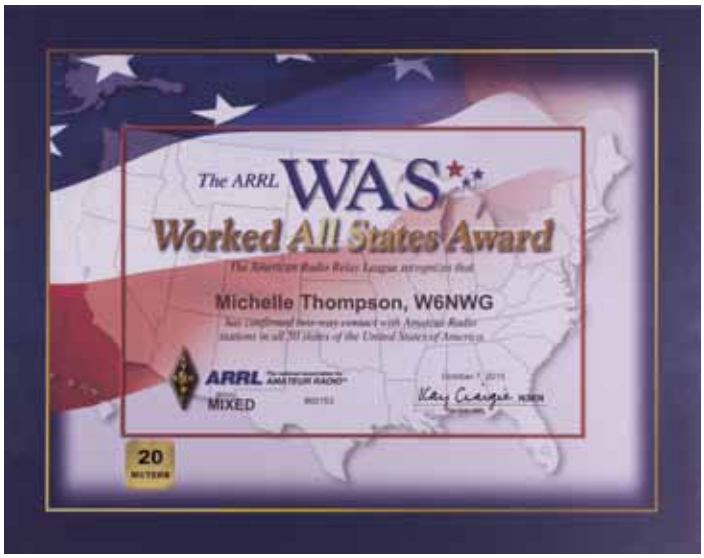
What could go wrong?

1. Weather may not cooperate. It's supposed to be windy and raining tomorrow and we are in a small tropical storm right now. The captain already told us we will be at Mt Athos at 0500z instead of 0700z as planned
2. The Zodiac could miss the rendezvous - very possible especially with the weather and the change of schedule.

3. The local authorities could be waiting for us to prevent a landing - unlikely (Free KY6LA fund for Bail soon)
4. The wifi hotspot could be out of range of a 3G or 4G signal. (Most likely) albeit I have had very good results with the outside gain antenna. Or the 3G connection could be just too slow or unrealizable.
5. A myriad of technical glitches either at my end or in La Jolla...not likely as it worked 100% from Skiathos today.
6. 20M propagation from La Jola will suck. probably great to VK at that time.

So please listen for me and hope I make it

I need at least 1 Q from Mt Athos to make it from Country #26



Want to help PARC earn more awards?

Contact board@palomararc.org about using the club call sign in upcoming contests!

We aren't that far from getting several more shiny stickers!

Silent Key

11 February 2016

Dave Tennant KD6EBY was introduced to the club and ham radio by his Palomar Observatory co-worker Mike Doyle AB6QT in the early 1990s. Dave passed element 2 in November of 1991, and got his technician license in December of 1991. He was so enthusiastic about amateur radio, that he had lined up a dual-band radio before he took his exams.

Dave was repeater site power chair from at least 1995 until after 2008. In June of 2008, when we retired the old battery building, he helped me and many others clean out the building and assisted in retiring the old batteries. He made numerous trips up to the repeater site during this time to transition to the new battery bank, provided patient and good-natured guidance, freely shared his experience and expertise, and was genuinely fun to be around.

Batteries and power were not the only activities he was involved with. He participated in many aspects of the club, and was a valued mentor and friend.

Dave passed away 11 February 2016 from a heart attack. He was 80 years old.

At right, Dave Tennant was featured in a 2008 July Scope article about transitioning from the old battery building to the current one.

Dave Tennant KD6EBY helps clean out the old battery building at the repeater site work party on June 8th.

March 2016

About Our Theme


1945
1985
40. JAHRESTAG DER BEFREIUNG VOM FASCHISMUS
DDR 20
DDR 10
DDR 50


500
DEUTSCHE BUNDESPOST
RADIOTELESKOP
#43766279


DDR
20
TAG DES KINDES 1964
KLEMKE


125 JAHRE UIT
25
DDR
1990


20
DEUTSCHE BUNDESPOST BERLIN
1973


UMWELTVERWALTUNGSKONFERENZ 1978
DEUTSCHE BUNDESPOST
60


DDR
25
GESELLSCHAFT FÜR
SPORT UND TECHNIK


4S
50 JAHRE INTERPOL
REPUBLIK ÖSTERREICH
O. STEINERT
1973
W. PFEILER


DEUTSCHE BUNDESPOST
20
Deutsche Funkausstellung
Stuttgart 1965


20
20 JAHRE DEUTSCHER DEMOKRATISCHER RUNDFUNK
DDR


40
DDR

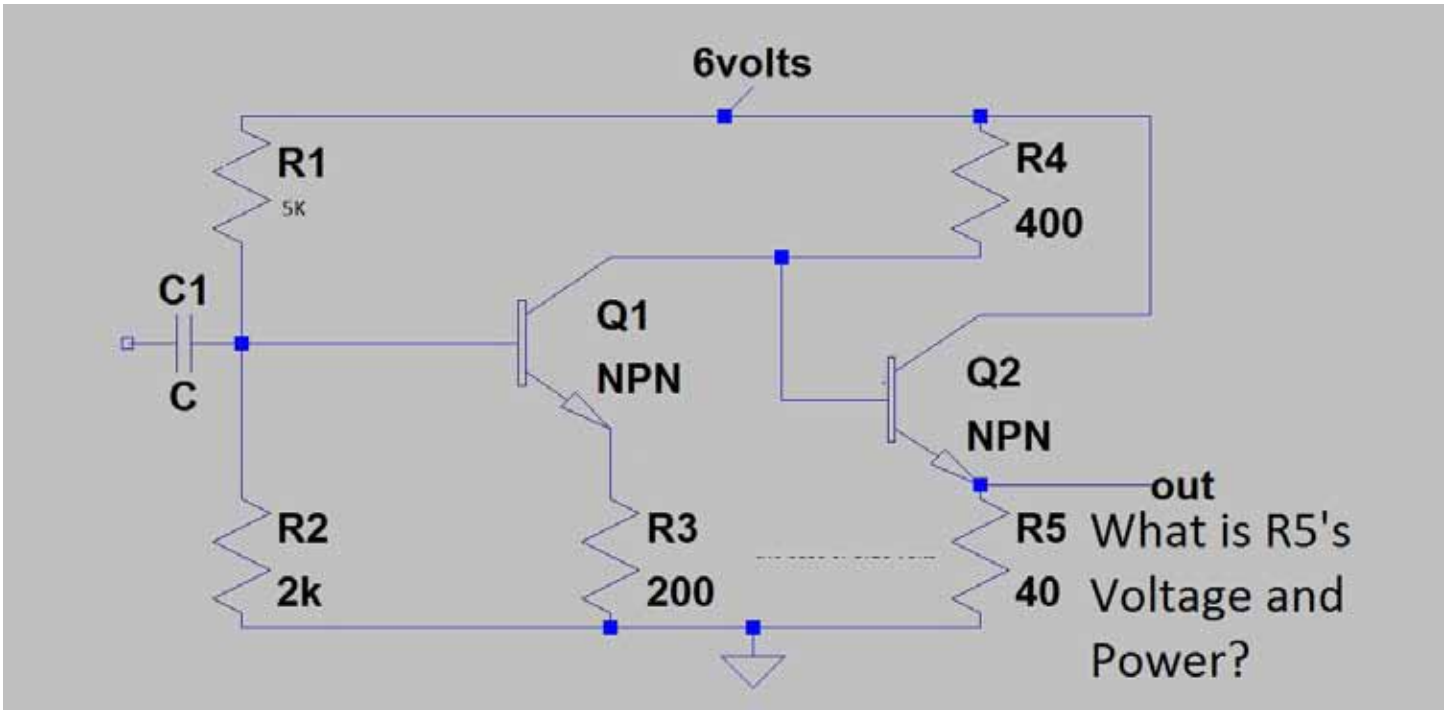

GESELLSCHAFT FÜR
SPORT UND TECHNIK
35
DDR

This collection of radio-related stamps is from East Germany (Deutsche Demokratische Republik is DDR), West Germany, and Austria (Österreich).

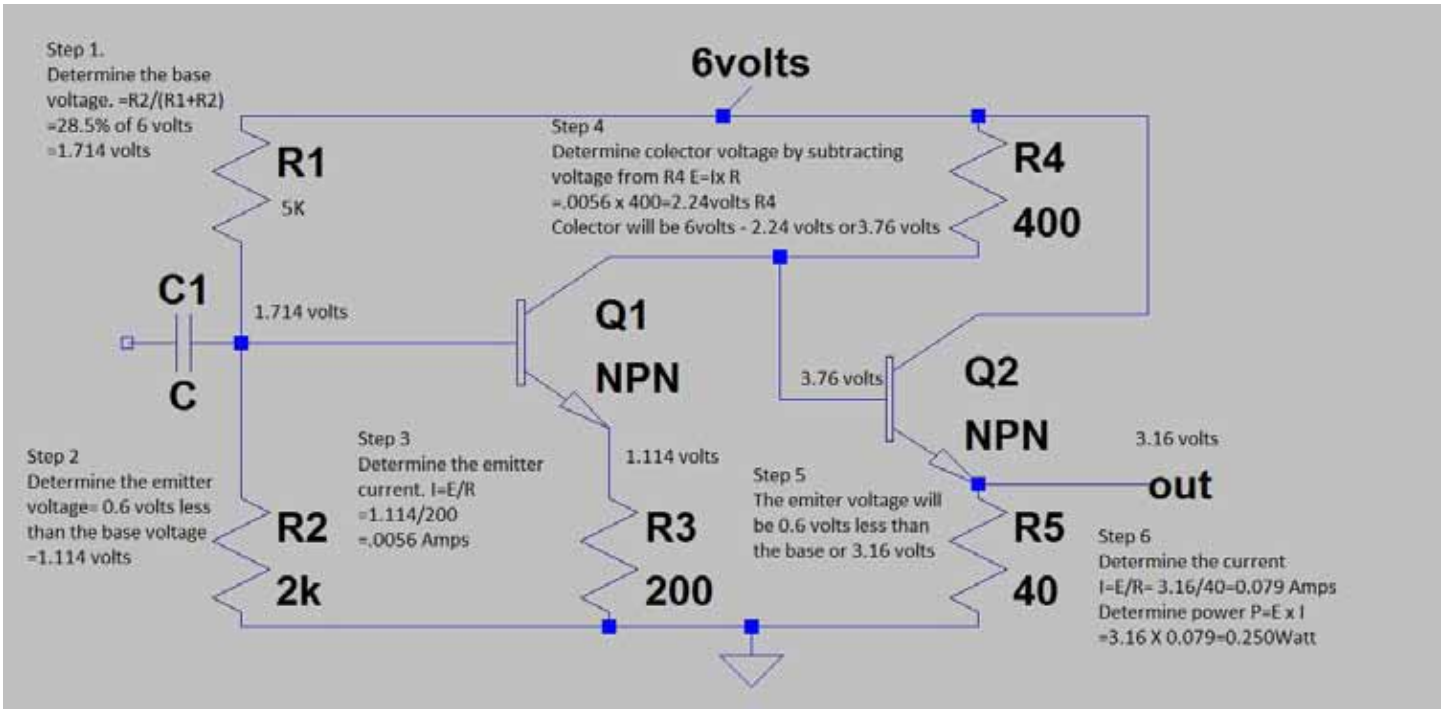
The emphasis on radio technology and science can be seen in the wide variety of stamps. When's the last time you saw a circuit diagram or an antenna on a stamp in the US?

March 2016

Want puzzle answer?



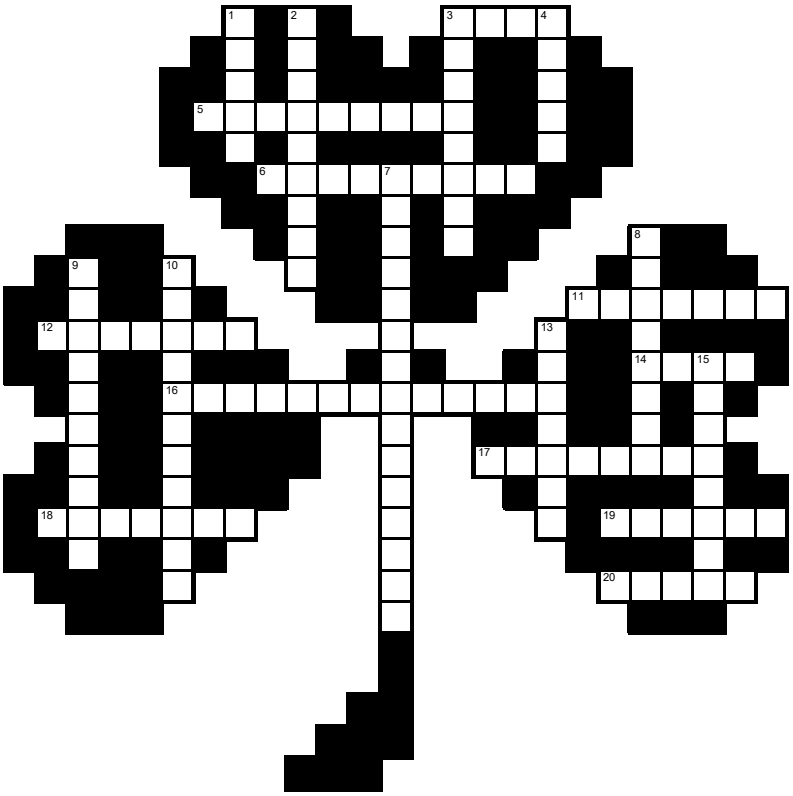
Puzzle from February Scope



Solution from puzzle author, Bill N6PIG

March 2016

Want puzzle?



Across

3 Apple spray (4)

5 Grow downward to a point of attachment (9)

6 Two minty lips! (9)

11 Blistered appearance. (7)

12 Bare leafless stalks are... (7)

14 Stop (4)

16 Terry Pratchett said, "His age was ..." (13)

17 No ham project is ever .... (8)

18 Extreme (7)

19 Fuzzy (6)

20 Holding one's piece (5)

Down

1 Kind of skeleton (5)

2 Attached at the base (9)

3 Genuine accessory seed covering (8)

4 In a manner that lacks gentleness. (5)

7 If you're a puffball, you're one of these (15)

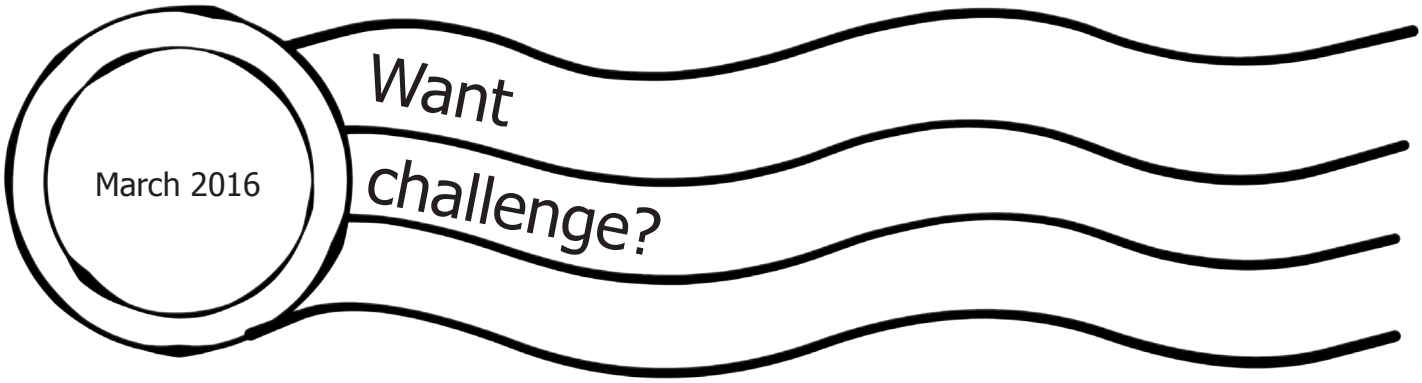
8 Resembling a calyx (8)

9 A double yolk would be ... (10)

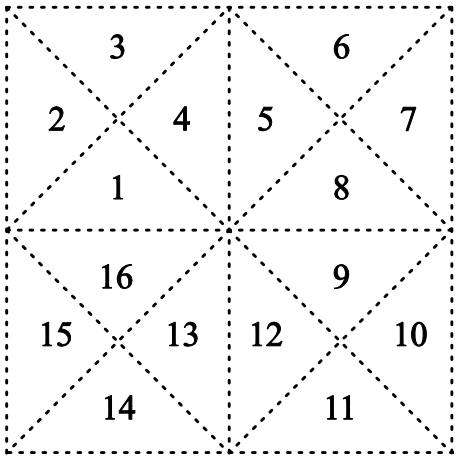
10 The category that parthenogenesis fits into. (11)

13 If it came from something, then it .... from something. (7)

15 Like a bunch of grapes (8)

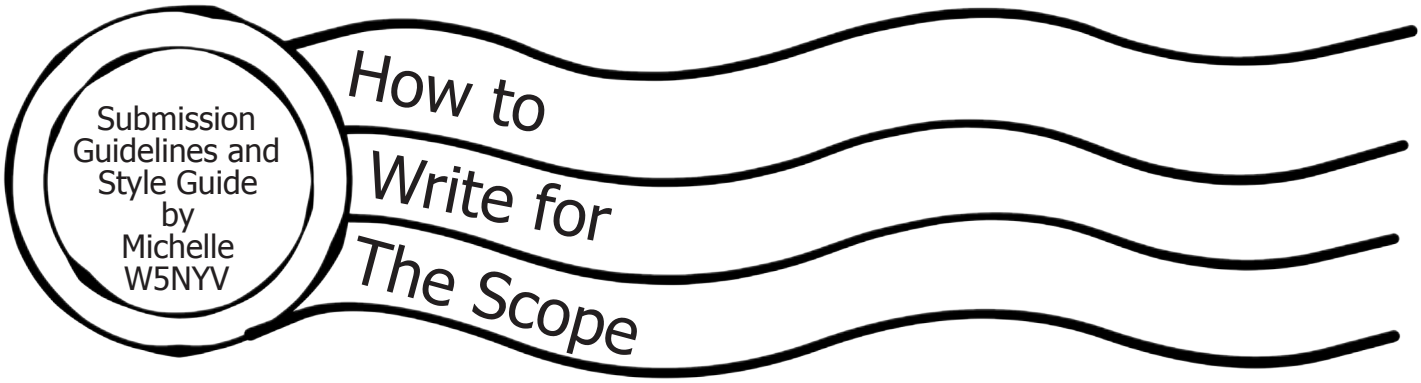


Stamp Folding Puzzle #3



Fold this block of isosceles right triangular stamps into a packet 16-deep with stamps in the following order:

4 1 16 6 5 15 14 8 7 13 11 12 2 3 9 10



Submission Guidelines

Article submissions in most modern file formats are accepted. Plain text in the body of an email, with attached full resolution photographs, is most preferred. Dropbox and several other file transfer services are supported.

Sending a fully-formatted PDF, so that the author can control formatting and exact wording, is also accepted. We use Tahoma font for body text, but will accept PDFs with other fonts. If any editing is necessary, then it will be negotiated with the author, and will then be the responsibility of the author.

For 2016, the Scope theme is postal marks and radio-related stamps. Postal theme artwork is welcome! Scans of amateur radio stamps, stories about stamps in general, interesting or quirky postal marks, fun things to do with the mail, puzzles about stamps, interesting stamp-related narratives, stories about current mail technology, QSL cards, QSL bureaus, and QSL collections are all very highly desired throughout 2016.

We want to publish articles about amateur radio and amateur radio related events and interests. Amateur radio covers a very broad swath of subjects. Contesting, technical experiments, narratives about the hobby, stories about how you became a ham, suggestions for an interview, ideas for more puzzles and games, experiences in community service, emergency communications, tours and travelogues of places of interest to amateur radio operators, mobile installation articles, ham shack articles, good operational practices, ideas for what PARC should be doing in 2016, and many other subjects are what we want to print in the Scope every month.

Articles that misrepresent a person, subject, or event will not be printed. Articles that are attack pieces, demean groups or individuals, or ridicule others will not be printed. The editorial staff of the Scope, in coordination with the Palomar Amateur Radio Club Board of Directors, has the final say on what is published in the club newsletter. Being a member of the club does not guarantee that a submitted article will be published. No payment is given in exchange for any article. Copyright remains entirely with the original author.

Style Guide

Time: Use 24-hour time in the following format.

"We started the event at 9:00 and began tear down at 16:00."

Name and Call Sign: Name is followed by call sign with no commas.

"Michelle Thompson W5NYV began writing the article."

After the first name and call sign is listed in an article, the style is to shorten it to first name and call sign with no commas.

"Michelle W5NYV was writing all day."

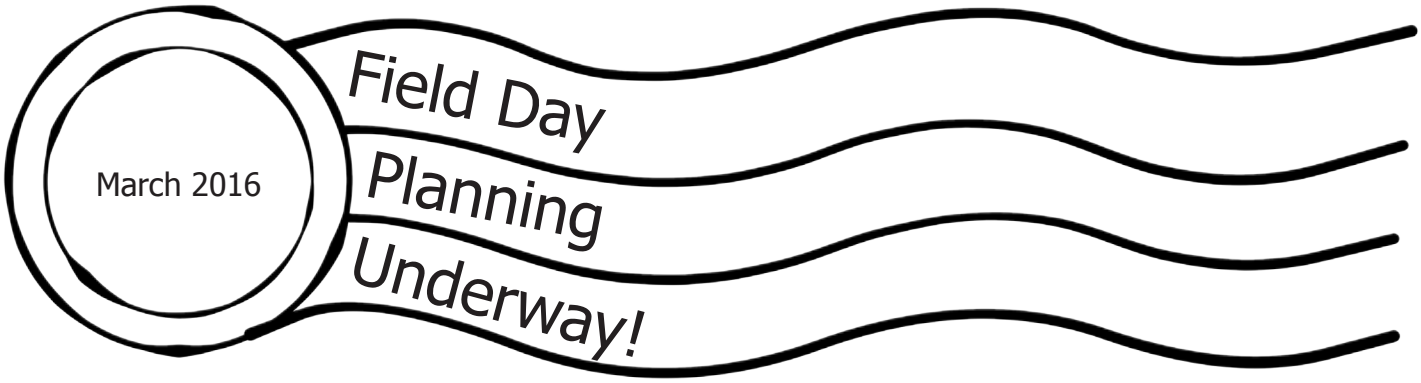
Do not use ellipses unless you know exactly how to use ellipses.

Ellipses… are not… the same thing… as a comma… or a pause...

Capitalization should be used for proper nouns. Proper nouns are the names used for an individual person, place, or organization. They are spelled with initial capital letters. For example, Michelle, New Mexico, and Boston Red Sox.

"And… that's it! That's All there is To It!"

What's the next step? Write an article, or propose one. If you need help, just ask! Mail to: scope@palomararc.org



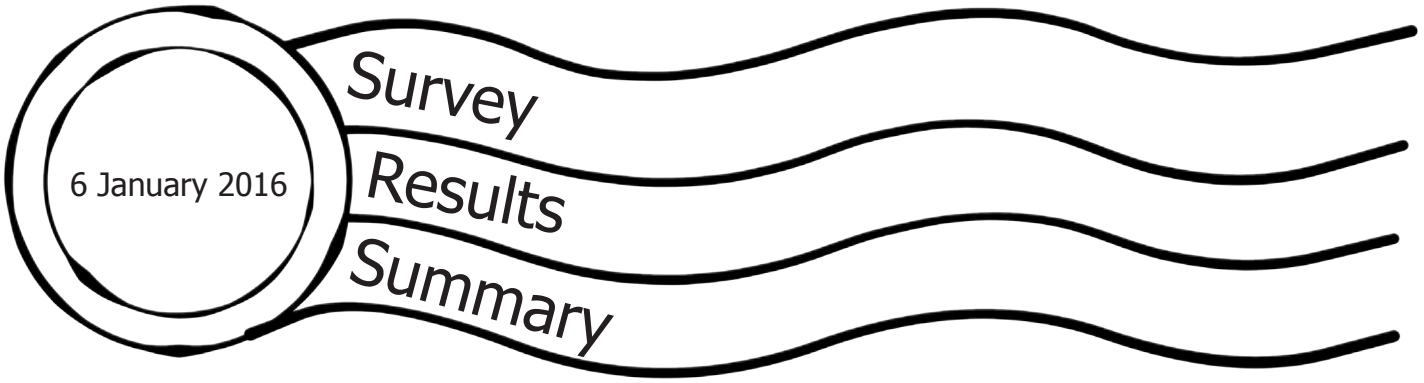
The Club's Field Day site is already reserved. The location is the corner of Valley Center Road and Lilac Road. Other logistics are on order. The Fire Department is arranged to fill the barrel counterweights, food services are planned, etc. In case you do not remember, Field day will take place June 24th. through 26th. Mark your calendars to participate, to help set up, or just come out to see PARC's FD operation. As in the past, the Club will begin set-up of the FD site on Friday, June 24th. Feld Day radio operations will start at 11:00 AM on Saturday morning the 25th., and will end at 11:00 AM on Sunday 26th.

FD site will be serving the great tri-tip BBQ for lunch on Saturday, and having excellent breakfast on Sunday. Everyone is invited to attend, and hopefully participate and operate during the FD period. You do not have to operate a station to enjoy the BBQ. Just come out and support the event. In preparation for FD there will be several work parties to prepare the FD equipment.

The first work party is planned for March 20th at the Tow Wizard site where the Club's equipment container is located. The work will begin at 9:00 AM and conclude about 2:00 PM. This first work party will inspect all the equipment, and any deficiencies found will be subject to a work plan to repair. In event of missing pieces or parts, they will be ordered after the work party. Then, installation of the ordered material and the final check out of all the hardware in preparation for FD will be done on a work party planned for May. A specific date will be announced in April.

Volunteers are invited to help with the inspection. This is a great chance to get out and have fun working with radio equipment. An excellent time to get the hands dirty working on real equipment, and learning about all those pieces and parts that make ham radio so much fun.

Please plan on joining the workparty. Contact NN3V or KF6WTN to sign up for the work party. All club members who volunteer for this will earn participation points that can be used in the Club's annual picnic prize drawing.



Attached is a brief summary of the results of the informal survey conducted at the January 6th., 2016 General Club Member meeting.

There were 35 survey forms distributed in the meeting. 24 responses were received in return. The survey responses reflect the comments of 69% of the attendees as there was no effort to make sure none of the meeting attendees left the meeting without returning the survey. The summary shows the collective response ratio among the 24 responses received.

This informal survey was intended as a means of learning about Club member nterests. The Palomar Amateur Radio Club Board of Directors will consider the answers as a way of identifying things you are interested in doing. Our objective is to plan Club activities and programs that will benefit you, and make PARC a club where your interests about our hobby are enhanced. Use the back of this form to add any further comments.

Please answer the questions in a manner that gives good understanding of your interests.

1. Are you active on the ham bands? Yes: 23; No: 1

2. If active, what bands and modes do you use? (List all that apply).
   HF + VHF/UHF 13
   HF 4
   Microwave/HF/VHF/UHF 6
   No answer: 1

3. Do you participate in PARC activities? Yes 19; No 3; No response 1.

4. If you do, in which club activity have you participated? (List all)
   No responses.

5. If you have not, or do not participate in Club activities, why not?

Yes: Maybe 1, as the "Yes" was not checked, but gave a reason as follows:
One respondent did not check the yes, but wrote that he or she was a tech and was not sure they could work the bands. Answer seemed associated with later answer that hams need more elmering.

No:
Live Out Of Area
Work Interferes / Work Conflicts: (2)
Events should be marketed

Survey results continued next page

6. What club activities do you wish the club to sponsor that would improve or motivate your participation?

a. Activities that cause us to use radios. Need to do so while hiking, or outdoor activities.
b. More operating days and more outreach.
c. Need more mentoring.
d. Have genuine elmering that encourages new hams to participate.
e. SDR demonstrations. The experimentation and digital ATV.
f. Hands on activities.

7. Of the following possible activities, in which would you actively volunteer and participate?

a. Field day preparations (equipment maintenance, antenna tuning, etc.) 12
b. Writing Scope article about your favorite ham radio subject 8
c. Participate in a PARC subcommittee Yes 8

Which one? :

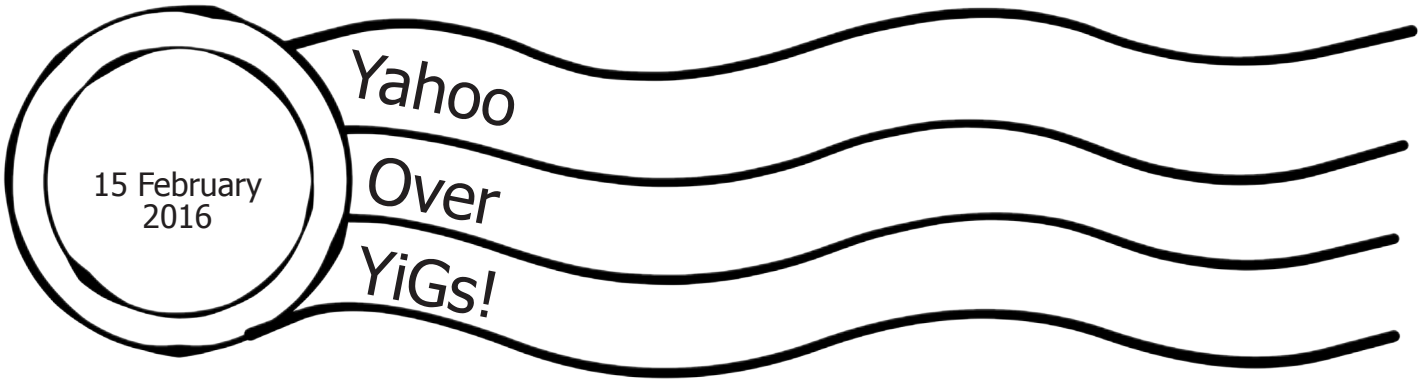
Technical 3
As needed 1
Remote Site 1
ARRL Scholarship 1

Conclusions: From a limited survey it is not wise to draw general conclusions. However, as far as the small population of Club member attendees at the meeting (after all, it was a night of severe winter storms in Southern California!), some preliminary conclusions are:

1. Club members are very active on all ham bands.
2. There is good participation in Club activities.
3. Respondents to the survey want more hands-on programs.
4. There is interest in getting genuine elmering.
5. PARC has to do better advertising about possible activities.
6. Field Day is popular.
7. Members are willing to participate in committees for specific functions.

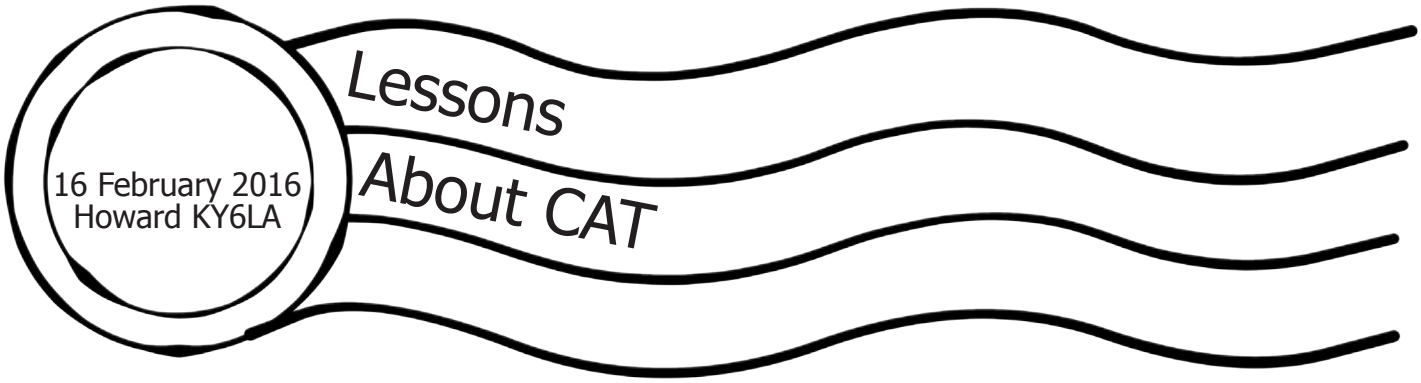
The PARC Board of Directors is reviewing future Club activities and planning programs to respond to this survey's general conclusions, limited as they may be.

The Board of Directors plans to carry out further similar surveys in order to get better focus on the kinds of activities and programs that are of interest to the Club's membership.



In the photos below Kerry Banke N6IZW demonstrates a YIG filter and YIG oscillator at the San Diego Microwave Group monthly meetup in February. YIG stands for yttrium iron garnet. This combination has some very interesting and useful magnetic properties. It has very high resistivity and a sharp ferrimagnetic resonance. When used in filters and oscillators, one sees excellent phase noise and very wide tuning ranges. This comes at the cost of large power requirements. YIGs tune slowly and require temperature control. And, as you can see from the detail photo on the left, they can be large.

For a lot more information:
http://www.vhfcomm.co.uk/A%20Simple%20Approach%20tyo%20YIG%20Oscil.pdf



Lesson 1 - CAT or Computer Aided Transceiver

Around 1980 with the advent of personal computers radio manufacturers decided that they could sell more radios if they allowed the radio to control peripherals such as Amps and even Personal Computers by sending and receiving frequency and mode data between the radio and peripherals

Unfortunately each manufacturer had his own idea of how this might work so we now have multiple different ways to connect the different radios to computers. Data Communications structures (languages) come from Yaesu, Icom. Kenwood, Flex Radio, Elecraft to name a few. They provide Band, Frequency, Mode and Control (TX, PTT) information but they are virtually incompatible so it takes a lot of work to make devices from different manufacturers to talk to each other. You end up needing a good traffic cop or translation service - which is what DDUTIL actually does for you ... so that you can get an Amp which reads one language to talk to a radio from a different manufacturer.

To further confuse and complicate the matter.the different manufactures use different communications mechanisms depending on when in history they started to implement CAT such as Parallel Ports (Yaesu - 1980), TTL Serial Ports (Icom - CI-V 1985), RS232 Serial Ports (Elecraft 1995), Firewire (Flex 2005) and Ethernet (Flex 2012) (Dates are best guesses)

Unfortunately most ham gear is stuck in the 1990's and still uses RS232 serial port communications even though it is very hard to find a computer today that still has RS232.

So basically CAT is a giant mess of incompatible languages and communications devices.

Around 1990 enterprising ham programmers started to make computer based logging programs that attempted to read the different radio protocols and extract frequency, band and mode data so that you could automatically log you r contacts. There are dozens of such programs around and by now most work with most radios as the programmers have figured out the different translators needed to make CAT work with their logger programs. Some very good ones are DXLab, HRD and Dogparksoftware. But by now everyone has his favorite and the debate is almost like religion as to which is the best..

In order to enhance the sales/acceptance of their products, innovative ham programmers started to include the ability to control other devices such as SteppIR, Rotors, Amps, Antenna Switches, Transverters, Wattmeters, etc. As you can imagine, each manufacturer of peripherals had a totally different CAT instruction set and communications device (RS232, Parallel Port, Ethernet) so again a good traffic cop like DDUTIL can make your life much easier.

We are now in the 2nd decade of the 21st Century.. most peripheral devices are still stuck in the 1990's but a few ar e entering the 2010's with Ethernet connections.. in the next couple of decades you can expect that Rs232 and Parallel ports will completely disappear to be replaced by Ethernet.

So it is very easy to understand why you are confused.. The ham communications (CAT) is still very much a big mess...

Lesson 2 - SmartCAT and DDUTIL

As I indicated in Lesson 1, the ability and mechanisms to connect a radio to a computer changed over time. Early radios used 3V TTL (Icom CI-V) to connect their radios to their amplifiers to send band data. But computers used more modern connections such as Serial Ports (RS-232) and Printer Ports (Parallel - eg. Yaesu Quadra) to communicate. This would have been OK if computer technology stayed static as most peripheral vendors started to standardize on RS-232 connections.

Unfortunately for Hams but fortunately for the rest of the world, computer technology keeps on changing and improving as the very slow speeds of RS232 were just not adequate to communicatre with modern devices... RS232 was soon replaced by USB ports on Computers. Parallel Printer Ports and RS232 Ports have almost completely disappeared. By the mid 2000's started seeing even USB device s evolve into USB2 and USB3 standard and ultimately most devices in the world except of Ham Peripherals seem to have become Ethernet or IP friendly.

To make matters worse for Hams most Ham Logging and Control Programs still operate in the 1980s in that they expect serial ports to communicate with the peripheral equipment and from the radio itself

So what do you do if you still own all that ancient ham peripherals stuck with 1980's serial ports when you cannot buy a computer today that has them..

Programmers invented Virtual Serial Ports to use "imaginary" ports inside their computer to replace all the physical ports that they now needed but could not buy anymore. There are a number of programs that do this such as Com0Com and VSP manager with varying degrees of complexity

What becomes really hard to understand is the concept that a Virtual Serial Port really needs 2 ends to it - just as if it were a real physical cable. .

To get the radio information:

One end is connected to the radio itself (in this case SmartSDR) and one end is connected to the computer program that collects the information for the logging program. Just to make sure you are totally confused you need to give a different Port Number to each end of the Virtual Serial Cable... e.g Port # COM6 and Port# COM106

To have the computer logging program send information to your other programs you also need virtual serial cables to connect the logger program and to the control program.

Now I assume you are really confused...

Well to make things even worse..... Enter Ethernet...a very fast way to communicate and much more powerful than any serial interface..

Ethernet does not operate as a Serial Port requiring two ends.. Instead the programmer assigns a two way port number (Like Port 4992) for the programs to talk to each other via a Telnet Connectio n...

Obviously the communications process for modern radios is very muddled...

So Flex had a Better Idea... SMARTCAT

SmartCat does a lot of stuff for you. It can create Virtual Serial Port Pairs for you. It can assign the Pairs to a specific Slice. It can create a PTT Port Pair for you. It can create a Telnet (TCP) port so you can communicate via Ethernet. It can create a Winkeyer Port so you can send perfect Morse Code. AND it has the ability to create ports for SO2R and other contesting protocols...

SmartCAT is just that much more powerful an interface system than anything we have seen before in Ham Radio

HOWEVER
The peripheral and Logging program and Digital Program guys are still for the most part stuck in the 1990's To exasperate the situation, as I mentioned before everyone has their own proprietary communications protocols. command structures, langua ges and even timings.. so it is still a big mess.

Enter _DDUTIL

Steve K5FR is a miracle worker.. He has spent years dissecting a large number of different peripheral. logging and digital programs and protocols.

DDUTIL - DATA DECODER UTILITY - takes the incredible disorganized ham radio communications mess and makes sense of it ... DDUTIL is the language translator, traffic cop and all knowing all seeing guru that allows you to connect everything together so that it works seamlessly so you don't even know DDUTIL is there. DDUTIL will connect you correctly to parallel ports, serial ports, Virtual Serial Ports and TCP - Telnet Ports so that each different device gets the right information.

Do you need to run DDUTIL all the time.. likely not as other bridging programs like SDRBridge do an excellent job with things like CWSkimmer

But, personally i run DDUTIL 100% of the time..

In theory Flex coul d add a lot of DDUTIL functionality to SmartSDR and it may happen one day But right now Flex has so many more things on its plate and DDUTIL is so easy to use and works so well that I doubt that there is much call for it except for remote Head installations...

Lesson #3 DAX

DAX means Digital Audio Exchange. But more on that later.

Ham Radio originally started with CW (actually Spark Gap) and then progressed to Voice. (AM, SSB and FM). However in the commercial world there as a need to transfer written text at speeds higher than CW speeds and with high degrees of accuracy.

Skilled CW operators were hard to find so where there was a need there was a solution.. The first solution was to develop landline teletype machines which quickly morphed into Radio Teletype Machines There was also a need to send pictures so we developed facsimile machines and other visible mechanisms like Hellschreiber..

How do these mechanical marvels send test over the air.. they mechanically and later electronically converted text into symbols which in turn were encoded with sounds so that they could be sent over the radio. From about the 1930's hams were s ending Radio Teletype Messages (RTTY) all over the world. .. you did not need to be a skilled CW to send text quickly and accurately.

So where does the word DIGiTAL come in...CW is really a digital mode.. it consists of Dits, Dahs and spaces... Every alphabetic character is represented by a series of symbols (Dits Dahs). The is true for RTTY except the coding is more complex (5 Level code representing each character consisting of up to 5 Marks and Spaces) and it uses 2 tones or frequencies rather than one like in CW. So to send RTTY you need to be able to quickly change the sending frequency to represent the correct sequence of marks and space tones.

For years this was accomplished by adding physical interfaces to your radio so that your keyboard could change the frequencies. These devices are called Terminal Network Controllers (TNC). Over the years TNC got more computing power so that eventually all you needed to do was send text to

the device and receive text from the device as the device did all the heavy lifting inside it.

Starting in the 1980's with the advent of Personal Computers, innovative hams started to use the computer's sound card to generate the needed tones to modulate and eventually decode RTTY signals. of course, there was a problem in that Audio tones from a computer do not easily match into a radio's microphone nor does the receive tones from the radio match into the Computer's microphone input.

This ultimately lead to the development of the Sound Card Interface which which is simply a device to match radio and computer sound cards together.

By about 2000 you had two competing technologies.. TNC - an external box to do the data translation for you and Sound Card Interfaces - an external box to match the radio to the sound card. As computers became more powerful and cheaper.. it became obvious that for most ham requirements the Sound Card Interface was a better solution. Plus the increasing processing power led to the advent of new modes like PSK, PACTOR,JT-65 with very significant advantages over RTTY. and CWSkimmer to replace human operator While adding these features to a TNC usually meant buying a new device - for a sound card interface it only meant adding new software to encode and decode.

With the advent of the SDR, it seemed to be rather redundant to decode a digital signal to analog audio output send it to a computer analog sound card input so that it could be digitized and decoded when the sound was already in digital format inside that computer.. Plus the decoding into analog sound and encoding that analog sound back into digital form adds noise and distortion to the signal causing degradation of the digital processing.

About 2005 Hams with SDR's started to keep the sound entirely in digital format inside the compute r.. BUT.. it's 2005.. the Ham Computer Programs such as CWSkimmer, PSK, HRD, WSJT all were designed for physical Sound Card Interfaces. Hence there was a need to create a Virtual Audio Cable to pretend to be a sound card interface to the digital computer programs. As far as the computer programs were concerned they were still dealing with computer sound cards even though now the entire signal stayed in digital form inside the computer.

There were many Virtual audio cables on the market. None were written specifically for ham radio needs but they worked OK with limitations. They were relatively complicated to set up and easily confused the beginners. Some worked better than others with different programs...By about 2012 there were a heck of a lot of support questions about interfacing the different virtual audio cables...

FLEX had a better idea for the 6000 series.

They created their own Virtual Audio Cable(VAC) and called it Digital Audio Exchange (DAX). DAX is much more powerful than most VAC as it has specific channels assignable to each radio receiver slice. PLUS DAX can handle very large data streams up to 192KHz in bandwidth compared to the usual VAC Maximum of 48KHz.

DAX has been designed specifically for Ham Radio Needs.. it provides an easy to use Virtual Sound Card interface from any specific radio receiver slice to any Digital Data program that can accept a sound card input. Very simply it replaces the computer sound card and the noise and distortion of an external sound card interface so that you get the best possible decoding and encoding of your digital data.

For more information you might want to read my
"Modern Radio - SDR 1010"

https://db.tt/0ALtyaj9

POOP! Still good Advice

April 1986
Packet Status
Register

PSR Quarterly
Volume 4 #19 April 1986

The Packet Status Register is published quarterly for $8.00 by the Tucson Amateur Packet Radio Corporation. Second-class postage paid at Tucson, AZ and additional mailing offices. POSTMASTER: Send address changes to TAPR, P.O. Box 22888, Tucson, AZ 85734.

This iconic article first appeared in 1986. The advice, aimed at packet operators, is still very good advice today for all digital modes.

Don’t be poopy!

Got an update or an opinion about all this BS?

Let us know
scope@palomararc.org

ELIMINATING POOP FROM PACKET

Peter Eaton, WB9PLW, and Lyle Johnson, WA7GXD

(Note: this material is being printed in PSRQ by popular demand. It may be considered offensive by some, to whom we apologize in advance. The message it contains, however, is very timely. Ed.)

Overview

A lot of POOP has been discovered on packet frequencies across the nation and around the world! Indeed, in addition to its health and welfare implications, POOP is both unnecessary and oftentimes offensive.

While other four-letter acronyms have been used to describe the characteristics of POOP, it is hoped that POOP is sufficiently recognizable by packeteers to eliminate the need to express the others!

What, exactly, is POOP? How does one eliminate it? How can one help others to cause it to not be propogated? The answers to these questions form the basis of this paper.

POOP - What is it?

POOP is simply an acronym for Poor Operating On Packet. While it may evoke other thoughts in one's mind, the relationship between those other thoughts and poor operating practices is probably pretty clear and will not be further elaborated upon.

POOP - How does one eliminate it?

In order to eliminate POOP, one must simply not generate it. If it is generated, it will be passed onto packet channels, needlessly clogging them.

While there are many varieties of POOP, and it would be impossible to describe them all in this paper, several of the more obnoxious and prevalent forms of it are described.

Frog POOP

If you have ever been around a pond, you have undoubtedly heard the loud and constant noise put on by frogs. It seems amazing that so small a creature can make such a disturbance!

If you have ever monitored a busy packet channel, you have probably seen plenty of beacon messages. Here again, a large disturbance may be caused.

Beacon features were included in TNC software in the early days of packet when stations were few and far between. Like the frog on the pond, the noises were made to attract attention of like species -- in this case, other packet stations. Unlike the frog, who settles down after he gets what he was looking for, many packeteers continue to send beacons, often on crowded channels.

Some packeteers contrive clever beacons, to sound bells, clear screens, or print multi-line declarations on the screens of all who can decode the beacon.

The proper rules governing beacons are simple:

1) Determine why you need to beacon.

Beacons declaring that you are unavailable, or on vacation, are perfectly useless and mark you as a real POOPer. If the information you are attempting to convey is important, perhaps leaving it as a message addressed to all on the nearest packet bulletin board station (PBBS) is a better alternative.

On the other hand, if you are living in tornado alley and see a funnel, an urgent beacon may be appropriate.

(In-search-of POOP)

If the purpose of your beacon is to let folks know you are around and want to connect, it may be better to just turn on the radio and let your TNC decode a few packets from other stations. This way you can see who is on and then simply send a connect request rather than a beacon.

Many new TNC software releases include an MHEARD function, allowing you to see the contents of a buffer containing the last several packet stations heard by your station.

If you are convinced that you must transmit without listening for a few minutes (or if the channel really does appear dead), dropping into UNPROTO mode (CONVERSE mode from COMMAND mode without first connecting) and typing a short CQ message (which may be as simple as a carriage return if UNPROTO is set to CQ) is preferable to beaconing one.

2) Compose the briefest possible beacon text.

Cute beacons that fill a screen, sound bells, or clear screens will only mark your station as obnoxious. It is a classic way to lose friends and increase your count of enemies!

3) Use the BEACON AFTER mode rather than BEACON EVERY.

If the channel is busy, one-way broadcasts (which is, after all, what a beacon really is) are not welcome. It's bad enough to try and maintain a connection through a digipeater or two without having having a channel clogged by transmissions from unattended stations that come on the air every few minutes. Beacon AFTER with a value of thirty minutes will assure that you do not add to busy channel bedlam.

4) Don't send beacons more often than every thirty minutes, preferably less frequently. (TNC 1 and TNC 2 users, B A 180 is the recommended setting.)

5) Digipeat beacons with care!

Digipeating may cause a large number of local packeteers to be subjected to screens full of your beacon text. This may be desireable. Then again, it may not. Consider your motive and objective for your particular beacon, then set up the path.

Squid POOP

As Amateurs, we admit to occasional spelling errors. We meant Scwid (Sending CWID)...

Sending a CWID is somewhat akin to using class B (spark) transmissions on the lower end of 20 meters when the band is open. It's annoying and serves no useful function.

The CWID feature was included in earlier TNCs to help the uninitiated masses of Amateurs identify a station that was making "packet racket." The decoder of the CW would (hopefully) contact the station sending the CWID and inform him of the strange noises eminating from his radio, upon which the proud packeteer would politely inform the bearer of the bad tidings that the noise was intentional. In the ensuing conversation and demonstration, another convert would then be won over to the new way of communicating.

Besides, the FCC once required a CWID every ten minutes or so!

Nowadays, the FCC has recognized our heretical behavior, packet is state-sponsored and CWID is no longer required of packet stations.

As a final note, most packet operation occurs on VHF, and everybody knows that most folks on VHF can't copy code anyway!

Bull POOP

Try entering a field containing a bull. While many bulls are mild mannered, some are very territorial and will chase you away.

The same is true of a packet BULLetin board station. Many are mild mannered, aware of other packet stations on the channel and content to share the channel with them.

Others, however, are not. They will chase you away unless you came to feed them.

They do it quite simply, and often are ignorant of their ferocity.

A skilled matador, however, can soon tame a ferocious bull. So can the operator of a PBBS tame his BULL.

The keys are TNC setup files. Most PBBS software contains a file (or files) describing the characteristics of the TNC(s) attached to the computer serial port(s). The magic commands are PACLEN, MAXFRAME and DWAIT.

If a PBBS is operating on HF, PACLEN should be fairly short, perhaps 40 or so. Since this parameter describes the length of the information field, not the header and control bytes, a setting in excess of 80 (the length of one line on most computer displays) is probably the longest needed.

MAXFRAME can be the cause of a lot of useful bandwidth reduction. If the PBBS is on a channel shared by other users, MAXFRAME 1 is reasonable. We have heard PBBS's sending packets of many frames to stations that were having a hard time decoding anything, and the channel was reduced to uselessness for other stations. Similarly, we have often heard PBBS's on HF sending long packets of multiple long frames, getting an ACK on the first one only (if any), and repeating the process over and over. Computers are infinitely patient, but humans wanting to use the channel may not be!

DWAIT is perhaps the strongest medicine to apply to an overly possessive BULL. PBBS stations should set DWAIT to 320 milliseconds. For a TAPR TNC 1 running 3.X software, this corresponds to DWAIT 6; for a TNC 2 it is DWAIT 32.

If you are not the owner of a BULL, but venture into territory where one lives, you can help tame the beast! The following suggestions are highly recommended:

1) DO NOT DX A PBBS! In this case, DX means multi-hop digipeating to a PBBS on VHF.

2) Don't send the PBBS a command before it has responded to your previous command!

Hitting a key twice (or hitting it harder!) WILL NOT improve your chances of getting through! The nature of a packet system is that the message gets through accurately, or not at all. Sometimes it may take a while, especially if a digipeater or HF link is involved, but it will get through. If not, you will get a
*** DISCONNECTED message.

Untimely POOP

POOP can't easily be made timely, but TNCs can! And TNC's that aren't timely can sure contribute to the level of POOP on a packet channel!

In the January, 1986 issue of PSR Quarterly, Tom Clark, W3IWI, made a convincing argument for the setting of the DWAIT parameter for all packet operations. His recommendations are:

User type	Time mSec	TNC 1 DWAIT	TNC 2 DWAIT
Digipeaters	0	0	0
Keyboard users	160	4	16
PBBS, Hosts	320	8	32
File Transfer	480	12	48

Digipeaters wind up with the highest priority. Since these stations are the most susceptible to collisions, and generate the most congestion on a retry, they deserve first shot at an empty time slot.

Keyboard users, operating in a keyboard-to-keyboard QSO, generate little traffic. After all, one can only type so fast! They get the next priority.

PBBS and host stations generally produce a fair amount of data out for a little data in. Thus, the keyboarder has priority getting into the PBBS, but the PBBS waits for other keyboard users before dumping what will probably be a longer packet onto the channel.

File transfers, generating the most data and hence requiring the most bandwidth, are requested to be more polite and give other users a fair shot at the shared channel. Thus, they are held off the longest.

Wide adoption of this scheme may not significantly reduce congestion on a channel, but it should help the channel operate on a fairer basis than otherwise.

Snake POOP

A snake has a fairly unique characteristic. A snake has no ears!

Too many packeteers seem to have the impression that, by connecting a TNC to the speaker jack on their radio, they don't have to have a speaker connected!

The results can often be observed. Excessive retries on a channel because the antenna isn't oriented properly, leading to multipath and poor reception. The other end of the link simply "goes away" for no apparent reason (unless you are listening!). The other station is over-deviating, or another user on another mode, or... And, on a shared-mode channel (or shared repeater), packet can get a bad name in a hurry!

Kangaroo POOP

A kangaroo jumps around. If you have long files to transfer, you should jump around, too!

A busy channel during the early evening hours is not the place for file transfers, automatic message forwarding or similar bandwidth-hungry procedures. What can you do? Jump off to another frequency, perhaps. If this is not feasible, set your alarm for 3 AM and jump to another time, eating up the channel then.

POOP - the final scoop

The ultimate means to eliminate POOP is to SCOOP! By means of the SCOOP, no one will ever be able to detect packet POOP emanating from your station!

SCOOP means Setting COrrect Operating Parameters. If you heed the advice to avoid POOP given above, this final measure will permit you to have a full clean-air rating!

Happy packeting!

TAPR Goals - 1986 Continued from page 1

Expect other positive action from this committee. And remember, they need your input! Write to the TAPR office, and mark the envelope ATTN: REGULATORY COMMITTEE.

Item 2, finding faster and better ways to communicate with the Amateur packet committee, led to another committee! This one is looking into, among other things, locating an economical electronic messaging service that can be accessed easily.

DRNET is one possibility. It has proved invaluable for coordination among the TAPR Board and Officers. The TNC 2 would not have happened without DRNET. And, while "free" accounts are limited, subscription accounts seem to be available.

The GENIE network, sponsored by General Electric, is also being investigated. Hopefully, the next PSRQ will contain details on the selected option.

Packet development issues, addressed by point three, led to the creation of the projects committee. Elsewhere in this PSRQ is an article containing guidelines for project submission.

Meanwhile, the NNC and high-speed radio/modem projects are underway. An HF tuning indicator semi-kit should be available at Dayton, based on the article by Dan Vester in the October PSRQ.

Got an idea? Let us know!

THE ONLY PORTABLE BASE STATION ANTENNA.

It works where others can't.

We packed a base station antenna into just 31". So it's the only one that's completely portable.

It carries its own ground plane with it. So you can set up your home base rig wherever you want. On boats, cars, campers, trucks. Or apartments with touchy landlords.

Our Portable Ground Plane Antenna (GP-400) offers performance virtually identical to larger, unsightly antennas. And on every surface, even fiberglass. It accepts peak power levels you expect only in bigger models.

A high-Q base coil provides maximum efficiency with really low VSWR. 1.25:1 or better.

Ours is a total system. Complete with sleek, new single-hole ground plane mount. And PL 259 connector, 16 feet of RG 58/u coaxial cable and adaptor. And a full 1 year warranty.

Ask for our antenna-to-go. Only $24.95 at dealers. Or for more information, write to us.

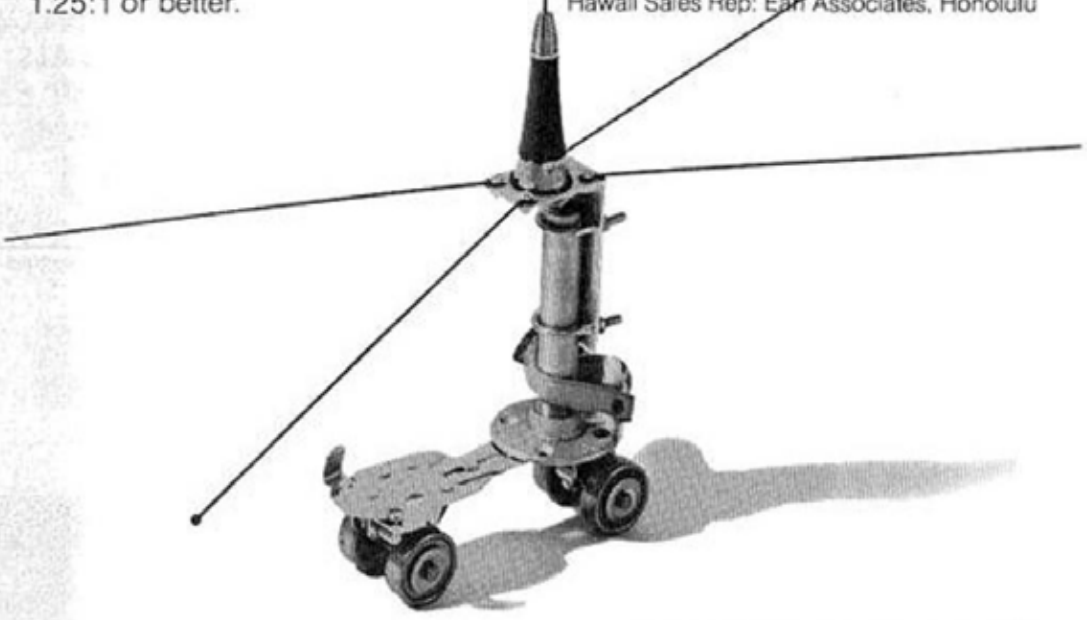
stinger

Unicom Electronics Corporation

8954 Mason Ave., Chatsworth, Calif. 91311

Dealers: call collect to order (213) 341-0044

Hawaii Sales Rep: Earl Associates, Honolulu



SDR Bits

March 2016
Michelle W5NYV

As my friend Frank AB2KT explains,

> "A software defined radio (SDR) design is where analog RF signals are digitized as close to the antenna as possible and everything else is accomplished by numerical calculations on the digital samples in real time."

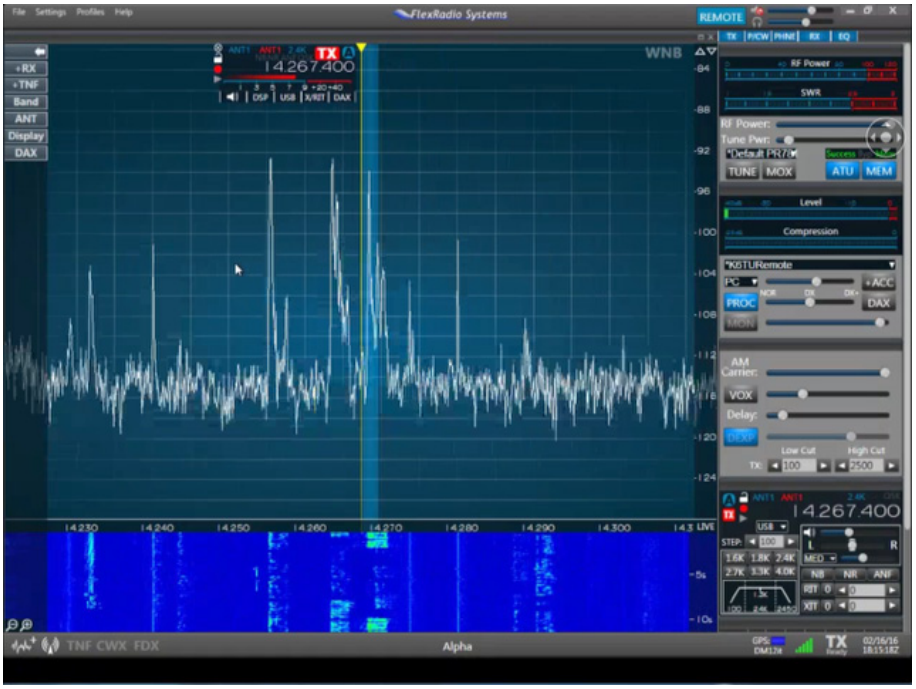
The power and flexibility of SDR lies in getting as much radio into digital circuits as possible. These digital circuits might be a general purpose processor, a field-programmable gate array (FPGA), or a graphical processor.

By substituting computer code for components, great flexibility can be obtained. Increases in flexibility come at the cost of complexity.

We've all encountered analog radios with too many bells and whistles and hidden or awkward controls. If an SDR is not presented to the operator through a quality user interface, then the digital equivalent of knobs and meters can be incomprehensible, unfindable, or unusable. With greatly increased capability, it's important to know what the SDR you're experimenting with is capable of, and how to access that capability.

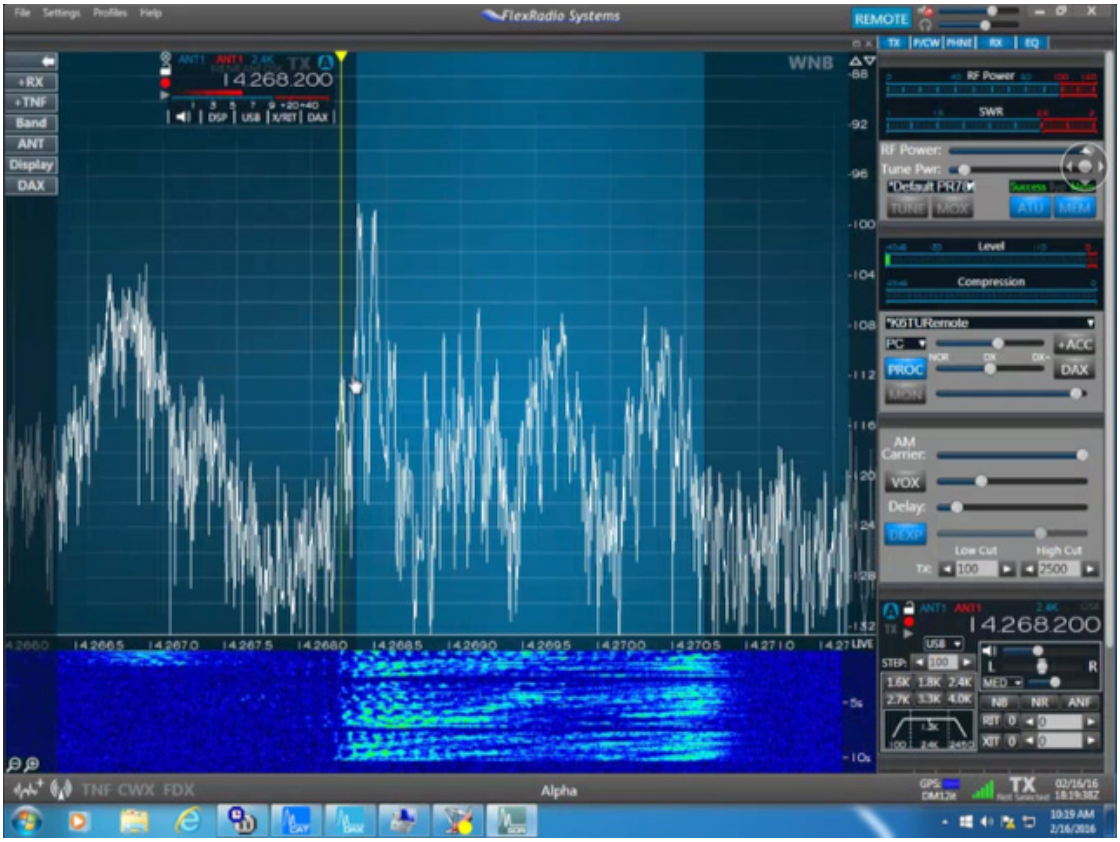
The current prevailing point of view is that the spectrum display, a graphical representation of the spectrum the radio can receive, is a necessary component of a quality radio.

SDRs without a spectrum display are described as "blind". Once accustomed to seeing the landcape of the radio spectrum, it can be difficult to go back to using radios that don't have it! Here's some examples that show the advantages of a spectrum display.

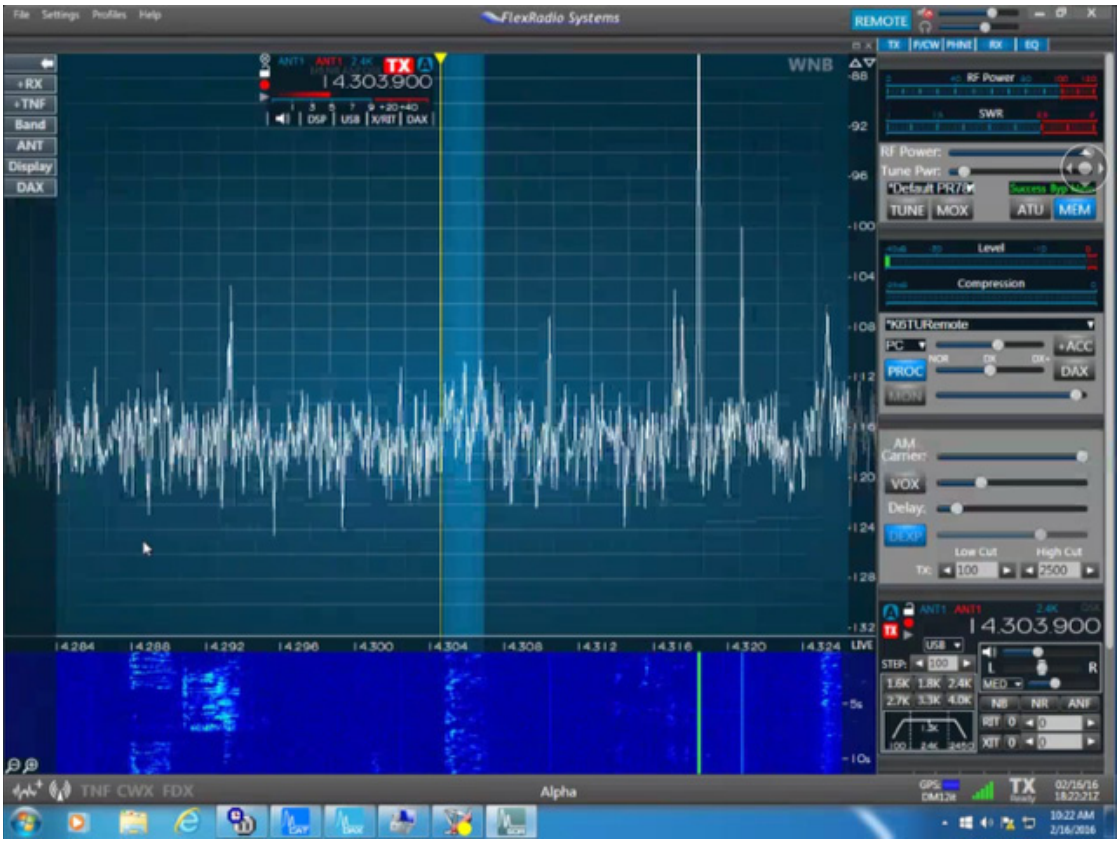


At left is a spectrum display from a Flex radio. This is from an ipad running the radio remotely.

You can see a number of strong stations but more interesting is the ability to see the weak ones.



Here is a shot of the operator zooming in on a signal.



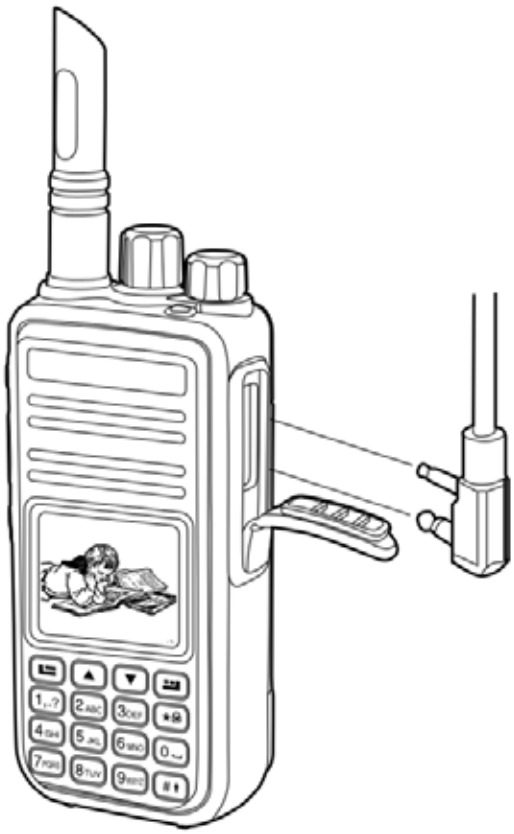
Here is a weak station that we can see because of the waterfall traces in the lower fraction of the screen. We would have likely missed this by spinning a dial. Now that we can see the station, we can listen and work the station.

Images and captions courtesy of Howard KY6LA

January 2016

Reverse Engineering the Tytera MD380

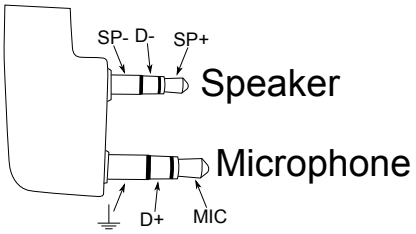
by Travis Goodspeed KK4VCZ,
with kind thanks to DD4CR and W7PCH.



The following is an adventure of reverse engineering the Tytera MD380, a digital hand-held radio that can be had for barely more than a hundred bucks. In this article, I explain how to read and write the radio's configuration over USB, and how to break the readout protection on its firmware, so that you fine readers can write your own strange and clever software for this nifty gizmo. I also present patches to promiscuously receive audio from unknown talkgroups, creating the first hardware scanner for DMR. Far more importantly, these notes will be handy when you attempt to reverse engineer something similar on your own.

This article does not go into the security problems of the DMR protocol, but those are sufficiently similar to P25 that I'll just refer you to *Why (Special Agent) Johnny (Still) Can't Encrypt* by Sandy Clark and Friends.[59]

8.1 Hardware Overview



The MD380 is a hand-held digital voice radio that uses either analog FM or Digital Mobile Radio (DMR). It is very similar to other DMR radios, such as the CS700 and CS750 from Connect Systems.[60]

DMR is a trunked radio protocol using two-slot TDMA, so a single repeater tower can be used by one user in Slot 1 while another user is having a completely different conversation on Slot 2. Just like GSM, the tower coordinates which radio should transmit when.

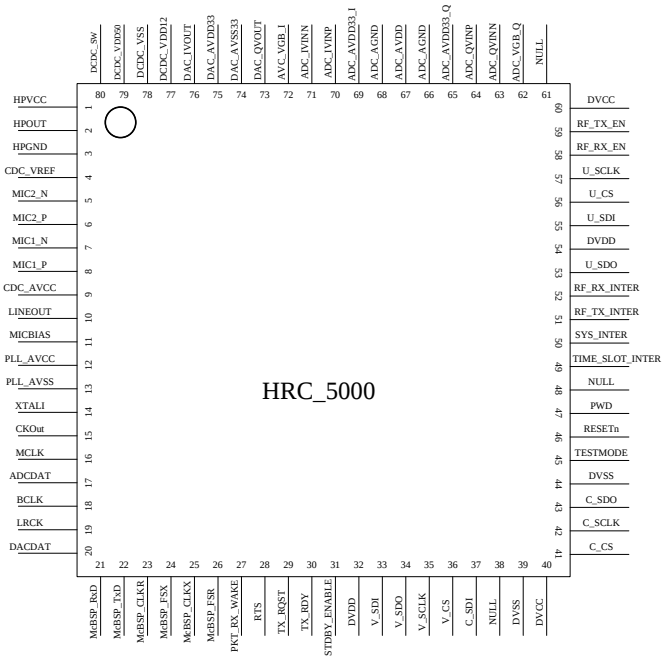
The CPU of this radio is an STM32F405 from STMicroelectronics. This contains a Cortex M4, so all instructions are Thumb and all function pointers are odd. The LQFP100 package of this chip is used. It has a megabyte of Flash and 192 kilobytes of RAM. The STM32 has both JTAG and a ROM bootloader, but both of these are protected by a Readout Device Protection (RDP) feature. In Section 8.8, I'll show you how to bypass these protections and jailbreak your radio.

There is also a radio baseband chip, the HR C5000. At first I was reconstructing the pinout of this chip from the CS700 Service Manual, but the full documentation can be had from DocIn, a Chinese PDF sharing website. 中国排名第一。

Aside from a bunch of support components that we can take for granted, there is an SPI Flash chip for storing the codeplug. "Codeplug" is a Motorola term for the radio settings, such as frequencies, contacts, and talk groups; I use the term here to distinguish the radio configuration in SPI Flash from the

[59] `unzip pocorgtfo10.pdf p25sec.pdf #from Proceedings of the 20th Usenix Security Symposium in 2011`
[60] The folks at Connect Systems are nice and neighborly, so please buy a radio from them.

code and data in CPU Flash.



8.2 A Partial Dump

From `lsusb -v` on Linux, we can see that the device implements USB DFU, most likely as a fork of some STMicro example code. The MD380 appears as an STMicro DFU device with storage for Internal Flash and SPI Flash with a VID:PID of `0483:df11`.

```
iMac% dfu-util -list
Found DFU: [0483:df11]
     devnum=0, cfg=1, intf=0, alt=0,
     name="@Internal Flash
           /0x08000000/03*016Kg"
Found DFU: [0483:df11]
     devnum=0, cfg=1, intf=0, alt=1,
     name="@SPI Flash Memory
           /0x00000000/16*064Kg"
```

Further, the `.rdt` codeplug files are SPI Flash images in the DMU format, which is pretty much just wrapper with a bare minimum of metadata around a flat, uncompressed memory image. These codeplug files contain the radio's contact list, repeater frequencies, and other configuration info. We'll get back to this later, as what we really want to do is dump and patch the firmware.

Unfortunately, dumping memory from the device by the standard DFU protocol doesn't seem to yield useful results, just the same repeating binary string, regardless of the alternate we choose or the starting position.

```
iMac% dfu-util -d 0483:df11 --alt 1 -s 0:0x200000 -U
      first1k.bin
Filter on vendor = 0x0483 product = 0xdf11
Opening DFU capable USB device... ID 0483:df11
Run-time device DFU version 011a
Found DFU: [0483:df11] devnum=0, cfg=1, intf=0, alt=1,
      name="@SPI Flash Memory /0x00000000/16*064Kg"
Claiming USB DFU Interface...
Setting Alternate Setting #1 ...
Determining device status: state = dfuUPLOAD-IDLE
aborting previous incomplete transfer
Determining device status: state = dfuIDLE, status = 0
dfuIDLE, continuing
DFU mode device DFU version 011a
Device returned transfer size 1024
Limiting default upload to 2097152 bytes
bytes_per_hash=1024
Starting upload: [####...####] finished!
iMac% hexdump first1k.bin
0000000 30 1a 00 20 15 56 00 08 29 54 00 08 2b 54 00 08
0000010 2d 54 00 08 2f 54 00 08 31 54 00 08 00 00 00 00
0000020 00 00 00 00 00 00 00 00 00 00 00 00 33 54 00 08
0000030 35 54 00 08 00 00 00 00 83 30 00 08 37 54 00 08
0000040 61 56 00 08 65 56 00 08 69 56 00 08 5b 54 00 08
...
00003c0 10 eb 01 60 df f8 34 1a 08 60 df f8 1c 0c 00 78
00003d0 40 28 c0 f0 e6 81 df f8 24 0a 00 68 00 f0 0e ff
00003e0 df e1 df f8 10 1a 09 78 a2 29 0f d1 df f8 f8 19
00003f0 09 68 02 29 0a d1 df f8 00 0a 02 21 01 70 df f8
... [same 1024 bytes repeated]
```

In this brave new world, where folks break their bytes on the little side by order of Golbasto Momarem Evlame Gurdilo Shefin Mully Ully Gue, Tyrant of Lilliput and Eternal Enemy of Big Endians and Blefuscu, to break them on the little side, it's handy to spot four byte sequences that could be interrupt handlers. In this case, what we're looking at is the first few pointers of an interrupt vector table. This means that we are grabbing memory from the beginning of internal flash at `0x08000000`!

Note that the data repeats every kilobyte, and also that `dfu-util` is reporting a transfer size of 1,024 bytes. The `-t` switch will order `dfu-util` to dump more than a kilobyte per transfer, but everything after the first transfer remains corrupted.

This is because `dfu-util` isn't sending the proper commands to the radio firmware, and it's getting the page as a bug rather than through proper use of the protocol. (There are lots of weird variants of DFU, created by folks only using DFU with their own tools and never testing for compatibility with each other. This variant is particularly weird, but manageable.)

8.3 Tapping USB with VMWare

Before going further, it was necessary to learn the radio's custom dialect of DFU. Since my Total Phase USB sniffers weren't nearby, I used VMWare to sniff the transactions of both the MD380's firmware updater and codeplug configuration tools.

I did this by changing a few lines of my VMWare `.vmx` configuration to dump USB transactions out

to `vmware.log`, which I parsed with ugly regexes in Python. These are the additions to the `.vmx` file.

```
monitor = "debug"
usb.analyzer.enable = TRUE
usb.analyzer.maxLine = 8192
mouse.vusb.enable = FALSE
```

The logs showed that the MD380's variant of DFU included non-standard commands. In particular, the LCD screen would say "PC Program USB Mode" for the official client applications, but not for any 3rd party application. Before I could do a proper read, I had to find the commands that would enter this programming mode.

DFU normally hides extra commands in the `UPLOAD` and `DNLOAD` commands when the block address is less than two. (Hiding them in blocks `0xFFFF` and `0xFFFE` would make more sense, but if wishes were horses, then beggars would ride.)

To erase a block, a DFU host sends `0x41` followed by a little endian address. To set the address pointer (block 2's address), the host sends `0x21` followed by a little endian address.

In addition to those standard commands, the MD380 also uses a number of two-byte (rather than five-byte) `DNLOAD` transactions, none of which exist in the standard DMU protocol. I observed the following, which I still only partially understand.

Non-Standard DNLOAD Extensions

`91 01`	Enables programming mode on LCD.
`a2 01`	Seems to return model number.
`a2 02`	Sent only by config read.
`a2 31`	Sent only by firmware update.
`a2 03`	Sent by both.
`a2 04`	Sent only by config read.
`a2 07`	Sent by both.
`91 31`	Sent only by firmware update.
`91 05`	Reboots, exiting programming mode.

8.4 Custom Codeplug Client

Once I knew the extra commands, I built a custom DFU client that would send them to read and write codeplug memory. With a little luck, this might have given me control of firmware, but as you'll see, it only got me half way.

Because I'm familiar with the code from a prior target, I forked the DFU client from an old version of Michael Ossmann's Ubertooth project.[61]

Sure enough, changing the VID and PID of the `ubertooth-dfu` script was enough to start dumping memory, but just like `dfu-util`, the result was a repeating sequence of the first block's contents. Because the block size was 256 bytes, I received only the first `0x100` bytes repeated.

Adding support for the non-standard commands in the same order as the official software, I got a copy of the complete 256K codeplug from SPI Flash instead of the beginning of Internal Flash. Hooray!

To upload a codeplug back into the radio, I modified the `download()` function to enable programming mode and properly wait for the state to return to `dfuDNLOAD_IDLE` before sending each block.

This was enough to write my own codeplug from one radio into a second, but it had a nasty little bug! I forgot to erase the codeplug memory, so the radio got a bitwise AND of two valid codeplugs.[62]

A second trip with the USB sniffer shows that these four blocks were erased, and that the upload address must be set to zero *after* the erasure.

`0x00000000 0x00010000 0x00020000 0x00030000`

Erasing the blocks properly gave me a tool that correctly reads and writes the radio codeplug!

8.5 Codeplug Format

Now that I could read and write the codeplug memory of my MD380, I wanted to be able to edit it. Parts of the codeplug are nice and easy to reverse, with strings as UTF16L and numbers being either integers or BCD. Checksums don't seem to matter, and I've not yet been able to brick my radios by uploading damaged firmware images.

The Radio Name is stored as a string at `0x20b0`, while the Radio ID Number is an integer at `0x2080`. The intro screen's text is stored as two strings at `0x2040` and `0x2054`.

```
#seekto 0x5F80;
struct {
  ul24 callid;    //DMR Account Number
  u8   flags;     //c2 private, no tone
                  //e1 group, with rx tone
  char name[32]; //U16L chars
} contacts[1000];
```

[61] In particular, I used r543 of the old SVN repository, a version from 4 July 2012.
[62] See PoC||GTFO 2:5.
[63] `http://chirp.danplanet.com`

CHIRP,[63] a ham radio application for editing radio codeplugs, has a bitwise library that expects memory formats to be defined as C structs with base addresses. By loading a bunch of contacts into my radio and looking at the resulting structure, it was easy to rewrite it for CHIRP.

Repeatedly changing the codeplug with the manufacturer's application, then comparing the hexdumps gave me most of the radio's important features. Patience and a few more rounds will give me the rest of them, and then my CHIRP plugin can be cleaned up for inclusion.

Unfortunately, not everything of importance exists within the codeplug. It would be nice to export the call log or the text messages, but such commands don't exist and the messages themselves are nowhere to be found inside of the codeplug. For that, we'll need to break into the firmware.

8.6 Dumping the Bootloader

Now that I had a working codeplug tool, I'd like a cleartext dump of firmware. Recall from Section 8.2 that forgetting to send the custom command `0x91 0x01` leaves the radio in a state where the beginning of code memory is returned for every read. This is an interrupt table!

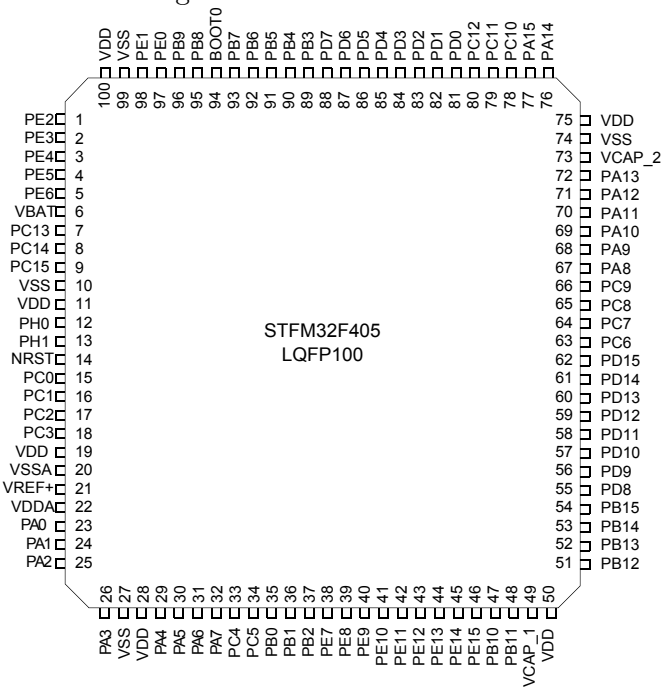
MD380 Recovery Bootloader Interrupts

`0x20001a30`	Top of the call stack.
`0x08005615`	Reset Handler
`0x08005429`	Non-Maskable Interrupt (NMI)
`0x0800542b`	Hard Fault
`0x0800542d`	MMU Fault
`0x0800542f`	Bus Fault
`0x08005431`	Usage Fault

From this table and the STM32F405 datasheet, we know the code flash begins at `0x08000000` and RAM begins at `0x20000000`. Because the firmware updater only writes to regions at and after `0x0800-C000`, we can guess that the first 48k are a recovery bootloader, with the region after that holding the application firmware. As all of the interrupts are odd, and because the radio uses a Cortex M4 core, we know that the firmware is composed exclusively of Thumb (and Thumb2) code, with no old fashioned ARM instructions.

Sure enough, I was able to dump the whole bootloader by reading a single page of `0xC000` bytes from the application mode. This bootloader is the one used for firmware updates, which can be started by holding PTT and the unlabeled button above it when turning on the power switch.[64]

This trick doesn't expose enough memory to dump the application, but it was valuable to me for two very important reasons. First, this bootloader gave me some proper code to begin reverse engineering, instead of just external behavioral observations. Second, the recovery bootloader contains the keys and code needed to decrypt an application image, but to get at that decrypted image, I first had to do some soldering.



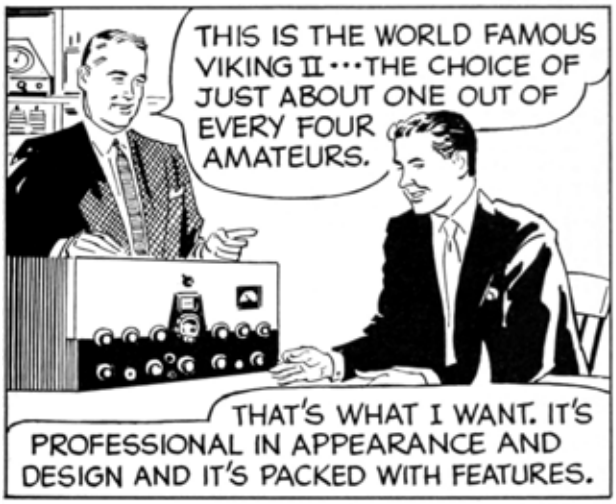
8.7 Radio Disassembly (BOOT0 Pin)

As I stress elsewhere, the MD380 has *three* applications in it: (1) Tytera's Radio Application, (2) Tytera's Recovery Bootloader, and (3) STMicro's Bootloader ROM. The default boot process is for the Recovery Bootloader to immediately start the Radio Application unless Push-To-Talk (PTT) and the button above it are held during boot, in which case it waits to accept a firmware update. There is no key sequence to start the STMicro Bootloader ROM, so a bit of disassembly and soldering is required.

This ROM contains commands to read and write all of memory, as well as to begin execution at any arbitrary address. These commands are initially locked down, but in Section 8.8, I'll show how to get around the restrictions.

[64] Transfers this large work on Mac but not Linux.

Thanks for that 5 by 9 plus, Algiers!
WE'RE USING A VIKING II HERE!



VIKING II TRANSMITTER KIT

- 10 Thru 160 Meters
- 180 Watts CW Input
- 150 Watts Phone Input

Available wired and tested, with tubes . . . or as a complete kit, the Viking II is today's most popular amateur transmitter.

Cat. No. **240-102.** Complete with tubes, less crystals, key and mike. **$279.50** Amateur Net

Cat. No. **240-102-2.** Wired and tested with tubes, less crystals, key and mike. **$337.00** Amateur Net

MAIL TODAY

E. F. JOHNSON COMPANY
288 Second Ave. S. W., Waseca, Minnesota

Please send me a copy of Catalog No. 714, containing a complete written and pictorial description of the Viking II.

NAME _____

ADDRESS _____

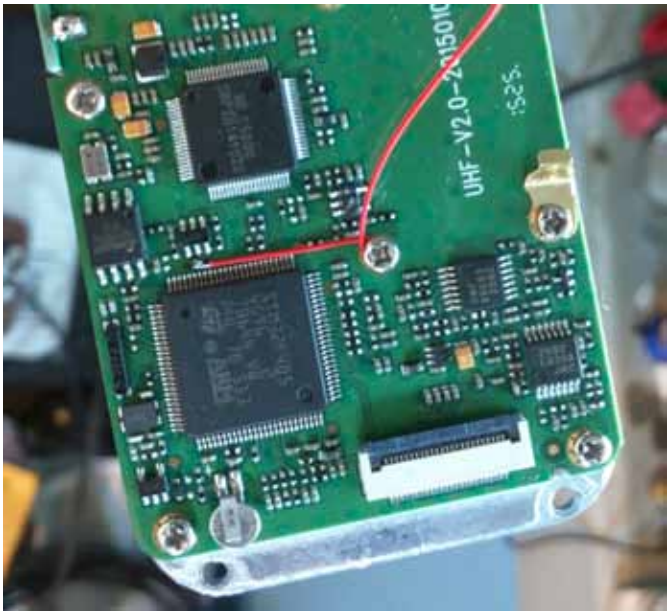
CITY _____ STATE _____

To open your radio, first remove the battery and the four Torx screws that are visible from the back of the device. Then unscrew the antenna and carefully pry off the two knob covers. Beneath each knob and the antenna, there are rings that screw in place to secure them against the radio case; these should be moved by turning them counter-clockwise using a pair of sturdy, dull tweezers.

Once the rings have been removed, the radio's main board can be levered up at the bottom of the radio, then pulled out. Be careful when removing it, as it is attached with a Zero Insertion Force (ZIF) connector to the LCD/Keypad board, as well as by a short connector to the speaker.

The STMicro Bootloader is started by pulling the BOOT0 pin of the STM32F405 high while restarting the radio. I did this by soldering a thin wire to the test pad near that pin, wrapping the wire around a screw for strain relief, then carefully feeding it out through the microphone/speaker port.

(An alternate method involves removing BOOT0's pull-down resistor, then fly-wiring it to the pull-up on the PTT button. Thanks to tricky power management, this causes the radio to boot normally, but to *reboot* into the Mask ROM.)



8.8 Bootloader RE

Once I finally had a dump of Tytera's bootloader, it was time to reverse engineer it.[65]

The image is 48K in size and should be loaded to `0x08000000`. Additionally, I placed 192K of RAM at `0x20000000`. It's also handy to create regions for the I/O banks of the chip, in order to help track those accesses. (IDA and Radare2 will think that peripherals are global variables near `0x40000000`.)

After wasting a few days exploring the command set, I had a decent, if imperfect, understanding of the Tytera Bootloader but did not yet have a clear-text copy of the application image. Getting a bit impatient, I decided to patch the bootloader to keep the device unprotected while loading the application image using the official tools.

I had to first explore the STM32 Standard Peripheral Library to find the registers responsible for locking the chip, then hunt for matching code.

```
/* STM32F4xx flash regs from stm32f4xx.h */
#@0x40023c00
typedef struct {
  __IO uint32_t ACR;      //access ctrl    0x00
  __IO uint32_t KEYR;     //key            0x04
  __IO uint32_t OPTKEYR;  //option key     0x08
  __IO uint32_t SR;       //status         0x0C
  __IO uint32_t CR;       //control        0x10
  __IO uint32_t OPTCR;    //option ctrl    0x14
  __IO uint32_t OPTCR1;   //option ctrl 1  0x18
} FLASH;
```

[65] The MD5 of my image is `721df1f98425b66954da8be58c7e5d55`, but you might have a different one in your radio.

The way flash protection works is that byte 1 of `FLASH->OPTCR` (at `0x40023C15`) is set to the protection level. `0xAA` is the unprotected state, while `0xCC` is the permanent lock. Anything else, such as `0x55`, is a sort of temporary lock that allows the application to be wiped away by the Mask ROM bootloader, but does not allow the application to be read out.

Tytera is using this semi-protected mode, so you can pull the `BOOT0` pin of the STM32F4xx chip high to enter the Mask ROM bootloader.[66] This process is described in Section 8.7.

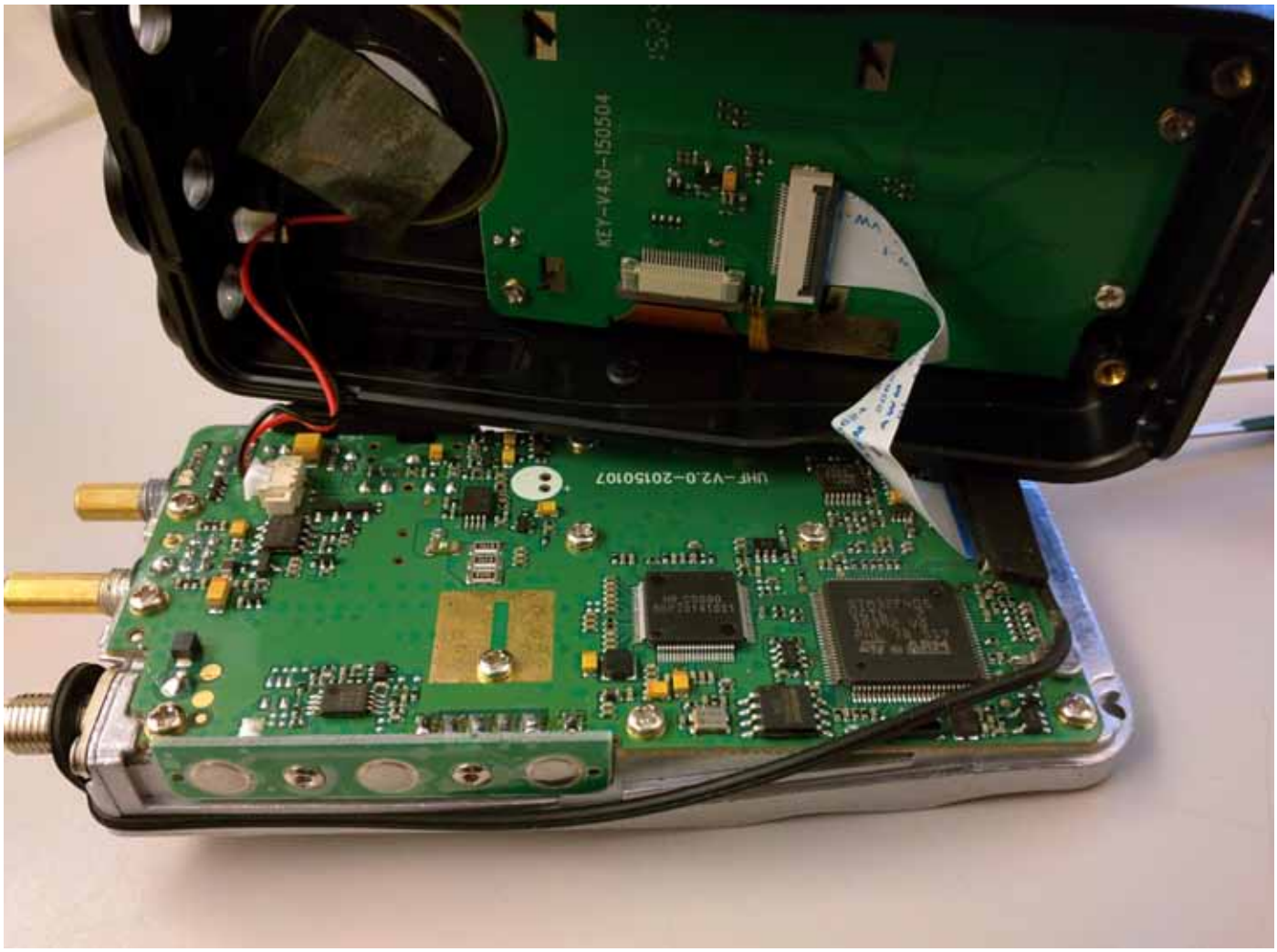
Sure enough, at `0x08001FB0`, I found a function that's very much like the example `FLASH_OB_RDP-Config` function from `stm32f4xx_flash.c`. I call the local variant `rdp_lock()`.

```
/* Sets the read protection level.
 * OB_RDP specifies the protection level.
 *        AA: No protection.
 *        55: Read protection memory.
 *        CC: Full chip protection.
 * WARNING: When enabling OB_RDP level 2
 *          it's no longer possible to go
 *          back to level 1 or 0.
 */
void FLASH_OB_RDPConfig(uint8_t OB_RDP){
  FLASH_Status status = FLASH_COMPLETE;

  /* Check the parameters */
  assert_param(IS_OB_RDP(OB_RDP));

  status = FLASH_WaitForLastOperation();
  if(status == FLASH_COMPLETE)
    *(__IO uint8_t*)
      OPTCR_BYTE1_ADDRESS = OB_RDP;
}
```

[66] Confusingly enough, this is the *third* implementation of DFU for this project! The radio application, the recovery bootloader, and the ROM bootloader all implement different variants of DFU. Take care not to confuse the them.



This function is called from `main()` with a parameter of `0x55` in the instruction at `0x080044A8`.

```
    0x080044a0     fdf7a0fd        bl rdp_isnotlocked
2   0x080044a4     0028            cmp r0, 0
,=< 0x080044a6     04d1            bne 0x80044b2
4   |  ; Change this immediate from 0x55 to 0xAA
    |  ; to jailbreak the bootloader.
6   |  0x080044a8     5520            movs r0, 0x55
    |  0x080044aa     fdf781fd        bl rdp_lock
8   |  0x080044ae     fdf78bfd        bl rdp_applylock
    `-> 0x080044b2     fdf776fd        bl 0x8001fa2
10      0x080044b6     00f097fa        bl bootloader_pin_test
```

Patching that instruction to instead send `0xAA` as a parameter prevents the bootloader from locking the device. (We're just swapping `aa 20` in where `55 20` used to be.)

```
iMac% diff old.txt jailbreak.txt
2 < 00044a0 fd f7 a0 fd 00 28 04 d1
            55 20 fd f7 81 fd fd f7
4 ---
  > 00044a0 fd f7 a0 fd 00 28 04 d1
6           aa 20 fd f7 81 fd fd f7
```

8.9 Dumping the Application

Once I had a jailbroken version of the recovery bootloader, I flashed it to a development board and installed an encrypted MD380 firmware update using the official Windows tool. Sure enough, the application installed successfully!

After the update was installed, I rebooted the board into its ROM by holding the `BOOT0` pin high. Since the recovery bootloader has been patched to leave the chip unlocked, I was free to dump all of Flash to a file for reverse engineering and patching.

8.10 Reversing the Application

Reverse engineering the application isn't terribly difficult, provided a few tricks are employed. In this section, I'll share a few; note that all pointers in this section are specific to Version 2.032, but similar functionality exists in newer firmware revisions.

At the beginning, the image appears almost entirely without symbols. Not one function or system call comes with a name, but it's easy to identify a few strings and I/O ports. Starting from those, related functions—those in the same `.C` source file—are often located next to one another in memory, providing hints as to their meaning.

The operating system for the application is an ARM port of MicroC/OS-II, an embedded real-time operating system that's quite well documented in the book of the same name by Jean J. Labrosse. A large function at `0x0804429C` that calls the operating system's `OSTaskCreateExt` function to make a baker's dozen of threads. Each of these conveniently has a name, conveniently describing the system interrupt, the real-time clock timer, the RF PLL, and other useful functions.

As I had already reverse engineered most of the SPI Flash codeplug, it was handy to work backward from codeplug addresses to identify function behavior. I did this by identifying `spiflash_read` at `0x0802fd82` and `spiflash_write` at `0x0802fbea`, then tracing all calls to these functions. Once these have been identified, finding codeplug functions is easy. Knowing that the top line of startup text is 32 bytes stored at `0x2040` in the codeplug, finding the code that prints the text is as simple as looking for calls to `spiflash_read(&foo, 0x2040, 20)`.

Thanks to the firmware author's stubborn insistence on 1-indexing, many of the structures in the codeplug are indexed by an address just before the real one. For example, the list of radio channel settings is an array that begins at `0x1ee00`, but the functions that access this array have code along the lines of `spiflash_read(&foo, 64*index+0x1edc0, 64)`.

One mystery that struck me when reverse engineering the codeplug was that I didn't find a missed call list or any sent or received text messages. Sure enough, the firmware shows that text messages are stored after the end of the 256K image that the radio exposes to the world.

Code that accesses the C5000 baseband chip can be reverse engineered in a similar fashion to the codeplug. The chip's datasheet[67] is very well handled by Google Translate, and plenty of dandy functions can be identified by writes to C5000 registers of similar functions.

Be careful to note that the C5000 has multiple memories on its primary SPI bus; if you're not careful, you'll confuse the registers, internal RAM, and the Vocoder buffers. Also note that a lot of registers are missing from the datasheet; please get in touch with me if you happen to know what they do.

Finally, it is crucially important to be able to sort through the DMR packet parsing and construction routines quickly. For this, I've found it handy

[67] `unzip pocorgtfo10.pdf hrc5000.pdf`

to keep paper printouts of the DMR standard, which are freely available from ETSI.[68] Link-Local addresses (LLIDs) are 24 bits wide in DMR, and you can often locate them by searching for code that masks against `0xFFFFFF`.[69]

8.11 Patching for Promiscuity

While it's fun to reverse engineer code, it's all a bit pointless until we write a nifty patch. Complex patches can be introduced by hooking function calls, but let's start with some useful patches that only require changing a couple of bits. Let's enable promiscuous receive mode, so the MD380 can receive from all talk groups on a known repeater and timeslot.

In DMR, audio is sent to either a Public Talkgroup or a Private Contact. These each have a 24-bit LLID, and they are distinguished by a bit flag elsewhere in the packet. For a concrete example, 3172 is used for the Northeast Regional amateur talkgroup, while 444 is used for the Bronx TRBO talkgroup. If an unmodified MD380 is programmed for just 3172, it won't decode audio addressed to 444.

There is a function at `0x0803ec86` that takes a DMR audio header as its first parameter and decides whether to play the audio or mute it as addressed to another group or user. I found it by looking for access to the user's local address, which is held in RAM at `0x2001c65c`, and the list of LLIDs for incoming listen addresses, stored at `0x2001c44c`.

To enable promiscuous reception to unknown talkgroups, the following talkgroup search routine can be patched to always match on the first element of `listengroup[]`. This is accomplished by changing the instruction at `0x0803ee36` from `0xd1ef` (`JNE`) to `0x46c0` (`NOP`).

```
for ( i = 0; i < 0x20u; ++i ){
  if ( (listengroup[i] & 0xFFFFFF)
       == dst_llid_adr ) {
    something = 16;
    recognized_llid_dst = dst_llid_adr;
    current_llid_group = var_lgroup[i+16];
    sub_803EF6C();
    dmr_squelch_thing = 9;
    if ( *(v4 + 4) & 0x80 )
      byte_2001D0C0 |= 4u;
    break;
  }
}
```

A similar `JNE` instruction at `0x0803ef10` can be replaced with a NOP to enable promiscuous reception of private calls. Care in real-world patches should be taken to reduce side effects, such as by forcing a match only when there's no correct match, or by skipping the missed-call logic when promiscuously receiving private calls.

8.12 DMR Scanning

After testing to ensure that my patches worked, I used Radio Reference to find a few local DMR stations and write them into a codeplug for my modified MD380. Soon enough, I was hearing the best gossip from a university's radio dispatch.[70]

Later, I managed to find a DMR network that used the private calling feature. Sure enough, my radio would ring as if I were the one being called, and my missed call list quickly grew beyond my two local friends with DMR radios.

8.13 A New Bootloader

Unfortunately, the MD380's application consumes all but the first 48K of Flash, and that 48K is consumed by the recovery bootloader. Since we neighbors have jailbroken radios with a ROM bootloader accessible, we might as well wipe the Tytera bootloader and replace it with something completely new, while keeping the application intact.

Luckily, the fine folks at Tytera have made this easy for us! The application has its own interrupt table at `0x0800C000`, and the RESET handler—whose address is stored at `0x0800C004`—automatically moved the interrupt table, cleans up the stack, and performs other necessary chores.

```
//Minimalist bootloader.
void main(){
  //Function pointer to the application.
  void (*appmain)();
  //The handler address is the stored in the
  //interrupt table.
  uint32_t *resethandler =
          (uint32_t*) 0x0800C004;
  //Set the function pointer to that value.
  appmain = (void (*)()) *resethandler;
  //Away we go!
  appmain();
}
```

[68] ETSI TS 102 361, Parts 1 to 4.

[69] In assembly, this looks like `LSLS r0, r0, #8; LSRS r0, r0, #8`.

[70] Two days of scanning presented nothing more interesting than a damaged elevator and an undergrad too drunk to remember his dorm room keys. Almost gives me some sympathy for those poor bastards who have to listen to wiretaps.

8.14 Firmware Distribution

Since this article was written, DD4CR has managed to free up 200K of the application by gutting the Chinese font. She also broke the (terrible) update encryption scheme, so patched or rewritten firmware can be packaged to work with the official updater tools from the manufacturer.

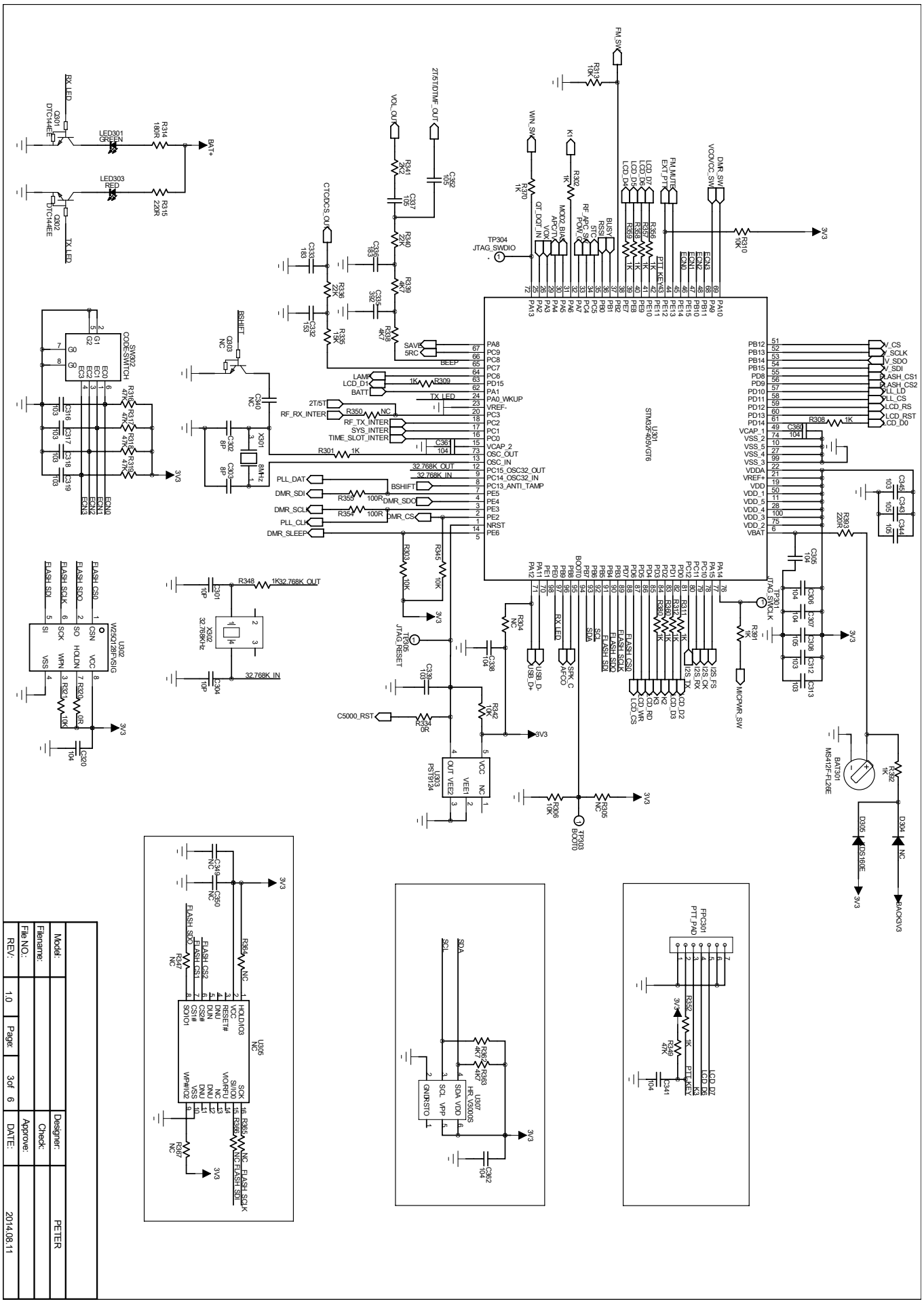
Patrick Hickey W7PCH has been playing around with from-scratch firmware for this platform, built around the FreeRTOS scheduler. His code is already linking into the memory that DD4CR freed up, and it's only a matter of time before fully-functional community firmware can be dual-booted on the MD380.

– — — – — — – — — –

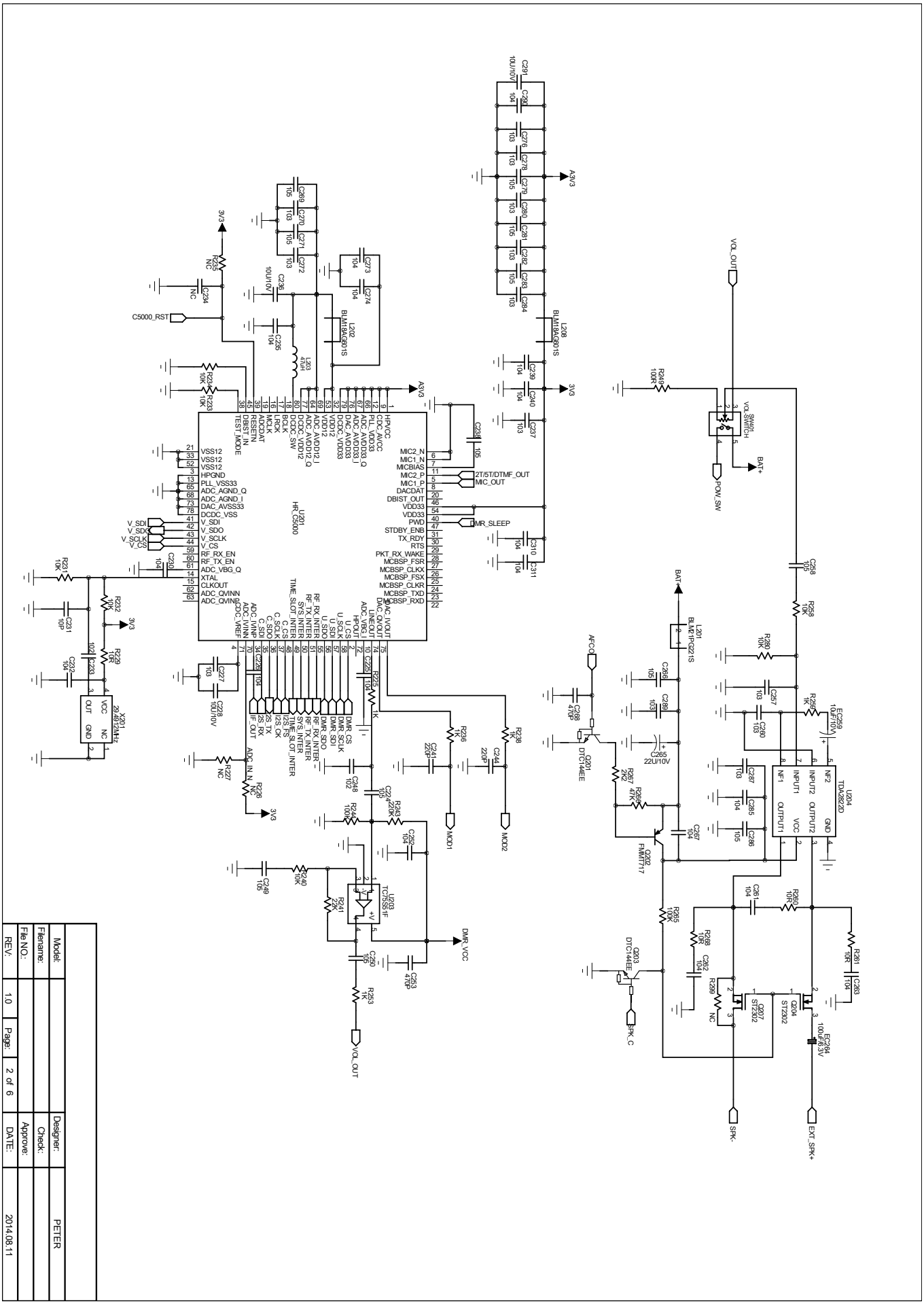
In this article, you have learned how to jailbreak your MD380 radio, dump a copy of its application, and begin patching that application or writing your own, new application.

Perhaps you will add support for P25, D-Star, or System Fusion. Perhaps you will write a proper scanner, to identify unknown stations at a whim. Perhaps you will make DMR adapter firmware, so that a desktop could send and receiver DMR frames in the raw over USB. If you do any of these things, please tell me about it!

Your neighbor,
Travis



Model:		Designer:	PETER
Filename:		Check:	
File NO.:		Approve:	
REV:	1.0	Page	3of 6
DATE:	2014.08.11		



Model:		Designer:	PETER
Filename:		Check:	
File NO.:		Approve:	
REV:	1.0	Page:	2 of 6
		DATE:	2014.08.11

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

PERIODICALS

Return service requested

Scope Volume #48 Issue #1 (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:

At 7:30pm on 2 March 2016, Palomar Amateur Radio Club will have a program about AREDN by Andre Hansen K6AH.

Come at 7pm to socialize. 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