HamGab

HAMFESTERS RADIO CLUB

January's meeting program will be given by Kurt, WB9FMC: He'll be talking about "basic antennas." We'll try to help you understand some of the basics by asking some questions: What is SWR? Who cares about impedance? What's to gain with a directional array? Grounds: Is it good for more than just coffee? Come join us for some fun and learning! See last month's HamGab for a complete preview. See you there!

PO Box 474
Crestwood, IL
60445-0474
www.hamfesters.org

Special Interest Articles

Passwords pg. 4
Shortwave pg. 5
Blue makes White pg. 5

January Birthdays

James W9ATT
Wanda W9CT
 Michael KC9OPV
Rudolph KA9EXP
Richard KA9HMV
Douglas W9IIX
John WØJLC
Thomas WY9M
Eugene WB9NAR
Bruno K9QKB
Jordan W9QKE
Lionel K2VSP
Michael WA9ZPM
William W9MJZ
Peggy K9QLM
Ruth Maloney
John K9JV

Officers

 President-Don KC9EQQ
Vice President –Jim KB9CYL
Secretary-Patty KC9LYE
Treasurer- ED WA9EOL
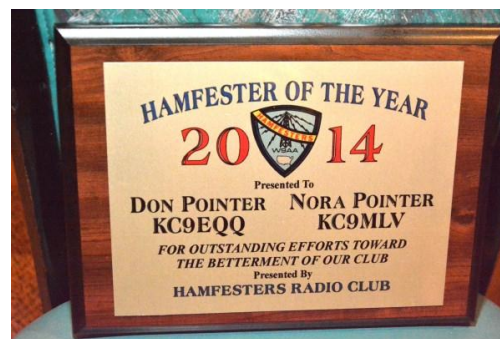SGT at Arm-Jim N9HSH
Trustee-Bruno K9QKB

Board Members

Nora KC9MLV
Steve W9KXT
Kurt WB9FMC
Kerry AA9SB
Cathy KC9NRH

Hamgab Editors

Steve & Eric
KC9OOL & KC9OOM
Scapstone@aol.com

HAMFESTER OF THE YEAR 2014 — Presented To DON POINTER KC9EQQ, NORA POINTER KC9MLV FOR OUTSTANDING EFFORTS TOWARD THE BETTERMENT OF OUR CLUB Presented By HAMFESTERS RADIO CLUB

Yes it's true. Our very own Don KC9EQQ and Nora KC9MLV are the Hamfesters of the year for 2014. It is truly a well deserved honor as Don and Nora are the heart and soul of the club. There isn't an aspect of the club that they aren't involved with and we all appreciate their hard work.. Congratulations Don and Nora! We had a great Christmas Party. The food was tasty, Bill the Band was excellent and the Hamfesters can't be beat for group of great people to spend an evening with. See the end of the HamGab for pictures.

DON'T FORGET TO GET YOUR SPLIT THE POT TICKETS AT THE NEXT MEETING!

A time for fewer words.......
But greater deeds......

A time to reflect on the years gone by
But to remember how we are blessed to have another year to meet up with, to plan for and to dream for better things throughout........

A time to look at more things as not just purely black and white
But with the delightful colors of hopes, dreams and Loving one another.......

A time to appreciate recognitions received
But more importantly, recognitions given.......

A time to realize how great a club can be matters not on its size
but on how great the people in it are.......

A time to realize there is a greater power that guides us, protects us, enriches us and loves us......

A time such as now to say thank you to those of you who are the fabric of our lives, who make lifes laughs last longer, its tears dry faster, and its ups and downs worth enduring.....

A time to receive so humbly (and gratefully so), the time honored tradition known as the Hamfester of the Year award........

good bye 2014 Hello 2015!

These thoughts are from Nora and I with the hopes you spread them to whom you love and will love in 2015. We know 2014 was tough for many, but let us as we enter 2015, forget the bad of 2014 and try to remember its good moments too. For that is what will allow us to openly embrace the colors and dreams of this new year known as 2015. God bless you all and we will see you at Kurt's program on Antennas on January 2nd.

It bears repeating: Nora and I wish to thank our fellow members Steve and Eric for selecting Nora and I to co-receive the Hamfester of the Year award for 2014. What an honor to be part of this special group of people who have received this outstanding award in years gone by and the years yet to come.

73 to everyone and God bless you all.

Don Pointer KC9EQQ

President of the best darn Ham Radio Club out there!

There was no meeting due to the Christmas party, so there are no minutes for this month.

Hamfesters VE Testing de Al Bukowski N9ZD VE Coordinator

Hamfesters VE Testing for December 2014
On December 13, 2014, Hamfester's Radio Club VE's team assembled to administered Amateur Radio exams at the Oak Forest City Hall. We had two Candidates who passed the Technician exam. Congratulations to the new Technicians. VE's who assisted me were Ron WB9JYZ, Tim AA9BV, Ron N9STU. Thank You to all the VE's for your dedicated time this past year.
Amateur Radio Exams INFO:
Hamfester's Radio Club VE's offer License Testing for those who want to get their first ham license, or those who want to upgrade to a higher class license. Examination sessions are available on the second Saturday of each month. We will assist you with completion of all necessary paperwork prior to taking your exam.
Requirements:
A fee of $15 dollars is charged for the examination. Payment is Cash ONLY. Please bring a government-issued ID; (one ID could be a driver's license). If you would prefer to not use your Social Security Number on your application, we suggest obtaining a Federal Registration Number (FRN) from the FCC website - otherwise you'll need to use your Social Security Number. If you do not remember the SSN, please bring your card.
Upgrade Examinations:
If you are already licensed and are taking an upgrade examination: Please bring your printed *original* license, and a copy of your current license that we can keep. Also, If you have recently taken an examination that has not been processed by the FCC, Please bring your *latest CSCE* and a *Copy of that CSCE* that we can keep.

Retaking the Exam:
If you almost passed the exam on your first try, and would like to try again, you may retake a different version of the exam for an additional $15 fee.
Morse Code Not Required!
Morse Code is no longer required for any level of amateur radio license. All Morse Code testing requirements for the Amateur Radio Service in the USA were eliminated on February 23, 2007.
Location and Time of Hamfesters VE administered Radio Exams:
Oak Forest City Hall 15440 S. Central Ave. Oak Forest, Il 60452. Doors open at 9:00 AM. We begin testing about 9:15 AM. Enter through the Police door entrance and look for the Amateur Radio testing exam signs for directions.
Our next test session will be held on Saturday January 10, 2015. (0900 hrs)
If you have any questions regarding our test session or about upgrading, please contact N9ZD via e-mail at: N9ZD@arrl.net.
Walk-ins are welcome and again test fee is $15.00 (cash only -- no credit cards or checks).

Like man, I hear Hamfesters is the "in" radio club these days.

Sony Corporation
New Headquarters

I heard Sony caved, but this is ridiculous!

Editor's Rambles

With companies left and right getting hacked these days, staying safe on the internet is more important than ever. One of the most important security practices is creating strong passwords, so let's take a look at how passwords get stolen and ways you can protect yourself.

Understanding how passwords get cracked can help you figure out how to beat the hackers. When you sign up for a website, your password isn't just stored in a file somewhere – that would be much too easy for a hacker to steal. Instead, your password is put through a special one-way function that turns it into a *cryptographic hash*. Putting the same password through the hashing function will always result in the same cryptographic hash, but it's impossible to reverse the cryptographic hash in order to get the original password. The website will then store the cryptographic hashes of the passwords knowing that when a user tries to log in, they can take the hash of their password and check it against the stored hash to see if the two match, but if an attacker steals the hashes, they won't be able to find the original passwords from the hashes.

Unfortunately, the hashing approach isn't perfect. Hackers can crack stolen password hashes because, as it turns out, computers have gotten fast enough that programs can be written to try hundreds or even thousands of passwords every second. The program might start by trying the password 'aaaaa' and seeing if its hash matches the stored hash. If it doesn't, the program will try 'aaaab' and 'aaaac' and so forth. Once the program finds a sequence of characters that produces the same hash as the one stolen from the website, the hacker will know that they've found that user's password. In the above example, if your password were 'abcde', it would take less than a second for the program to crack it!

What if you used a longer password? If the computer had to try six-letter sequences of characters, starting with 'aaaaaa' and going until it found your password, 'abcdef', it would in theory take it roughly twenty-six times longer because it needs to try all the possibilities for the added letter. However, this program is only looking at passwords composed of all lower-case letters – if you used 'Abcdef' as your password, it would never find it. This is because if you don't just limit yourself to the lowercase letters, there are even more possibilities the hacker has to try. When you add in the capital letters, there are now 26 more possibilities for each character. When you add numbers, that adds another ten, and symbols add another twenty or so. Instead of having to try all possible combinations of the 26 letters to figure out which is the correct password, the program now has to try all possible combinations of about 90 characters. 'Ab<d3F' would be a much more secure password than 'abcdef'. Unfortunately, computers are fast enough that eventually, they can try all of these more complicated passwords too.

The reason computers can try all the more complicated passwords is because hackers have taught them how to cheat at doing so. The standard advice has always been to only use passwords that mix upper and lower case letters and introducing number or symbol substitutions, but this scheme is falling out of favor in the security community because there are only a few common substitutions most people make, and hackers - along with the professional security experts and statisticians that work on password cracking tools - learned long ago how to predict substitutions in such a way that makes cracking such passwords only slightly less trivial than cracking other passwords. Respected security expert Bruce Schneier takes a look at it here: https://www.schneier.com/blog/archives/2007/01/choosing_secure.html
He suggests an approach based on compressed versions of personally identifiable phrases, but even this approach has come under fire. This polemic:
http://robinmessage.com/2014/03/why-bruce-schneier-is-wrong-about-passwords/
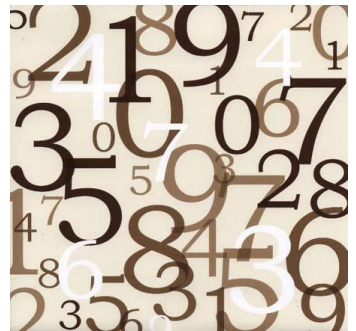argues that while the entropy of the passwords produced with the "Schneier scheme" may appear sufficiently high to automated tools, because they are created from English phrases, their information

density is too high for them to be considered strong passwords (to put it in simpler terms, they are insufficiently random, which means they are easier to predict). The safest password is of course a completely random string of characters of a substantial length, but such passwords are hard to remember without automated tools. Perhaps the only way to have a chance at protecting oneself is to mix a variety of password creation schemes (perhaps phrases with substitutions) in an attempt to fool the cracking programs for a little while longer. Nonetheless, the security community agrees on one thing: The age of passwords is rapidly ending, and soon new technologies will have to be adopted to protect users online.

One such emerging technology is two-factor authentication. Whenever you try to log in to a website with two-factor authentication enabled, the website will check your password, and if it is correct, it will then ask you for a code texted to your phone or generated by a special app. This is one of the most bulletproof ways to protect yourself; because while a hacker might steal your password, it's unlikely they'll also steal your phone. Not all websites offer two-factor authentication, but it's a good idea to turn it on if you're using a service that offers it. Google, Facebook, Chase, Bank of America, and Paypal all offer it, so if you want to add one more layer of protection to those accounts, it would be a good idea to enable it as soon as possible. Each site should have its own instructions for setting it up, and you can find a full list of services that offer two-factor authentication here: https://twofactorauth.org/

The two password links above talk a lot about "bits of entropy", a concept in information theory. Essentially, it's a way of conveying how much information something gives you in the forms of binary values. Password cracking programs work by attempting to guess your password, so the more bits of entropy, the more information they have to guess in order to find the right one. This is why a random string like 'ouepngia' has fewer letters than 'Password', but would probably have more bits of entropy because 'Password' appears in the dictionary. That's why if I give you the string 'P_s_w_rd' you can easily guess what the original was, but if I give you the string 'o_e_ng_a' it's much harder to get 'ouepngia' back out of that.

Mathematician Claude Shannon wrote two excellent papers on the subject,
http://cm.bell-labs.com/cm/ms/what/shannonday/shannon1948.pdf
http://languagelog.ldc.upenn.edu/myl/Shannon1950.pdf
but they're a bit technical for anyone without a background in formal mathematics.
XKCD has a surprisingly good run-down that explains it in plain terms, so I invite you to check it out (It only takes about three minutes and it's a fun read) if you want to understand the information theory terms discussed in the password articles a bit better.
https://what-if.xkcd.com/34/

As a bonus, here's a Microsoft security researcher's take on passwords. He says that it's important to keep in mind whether it matters if your password for a given site is compromised. Sometimes insecure passwords are fine for accounts that you don't care about.
http://www.pcworld.com/article/2455350/microsoft-researchers-use-simple-passwords-for-most-of-your-accounts.html

One liners…

Two antennas met on a roof, fell in love and got married.
The ceremony wasn't much, but the reception was excellent.
Since they were a perfect match, soon they generated harmonics. And wrapped the harmonics in dipoles. But later the harmonics turned out to be parasitic elements.   The true story: she was a tri-bander and he felt trapped, so they went on separate beam heading.
Courtesy of Brian W9HLQ

Milestone Shortwave Contact with Australia

A3BQ

The first direct two-way radio contact between A3BQ in Melbourne and U6AHP in the USA in 1924, helped open up the age of shortwave long distance communication. The breakthrough on 87 metres came during the transpacific tests run by the WIA Victorian Division in cooperation with the American Radio Relay League. The aim was to prove that signals could be detected and amplified sufficiently to communicate long distances. Ross Hull A3JU in Melbourne heard faint US signals through the static and is credited with being the first Australian to do so. But Max Howden A3BQ at Box Hill made the first contact with the USA using his now primitive home-built equipment. It was on November 2 that A3BQ made a contact with William L. Williams U6AHP, of Pomona California, USA. Max ran 130 Watts using a single-tube transmitter feeding a six wire antenna. His antenna consisted of six wires, 65 feet long and 80 feet in the air. The first trans-pacific QSO was a very significant achievement at a time when radio amateurs were seeking to prove that long-distance communication was possible on short wavelengths that governments had considered to be useless. Max went on to make further contacts. Nine days later he achieved the first Australia to UK two-way wireless telegraphy contact by working E. J. Simmonds, G2OD, in Buckingham, England. A telegram the next day confirmed the first Australia to England contact. Others repeated the feat. Until then everything was in Morse code, but byJanuary 1925, A3BQ was able to copy G2OD on telephony.

The efforts of Max Howden and many other pioneering radio amateurs of that era, both the southern and northern hemispheres, significantly added to the knowledge of communications. It led to the rapid development of radio in terms of inter-continental and global communications and opened up the short waves for broadcasting, international wireless telegraph and many other uses over long distances.

A January 1925 QST article reporting various successful contacts with Australia and elsewhere proclaimed, "the day of true international Amateur Radio is here". It also led to changes in callsign prefixes to clearly identify the country of origin, but originally A meant Australian, G was used in England, and U for USA. After a long career in wireless Maxwell Howden passed away in 1980.
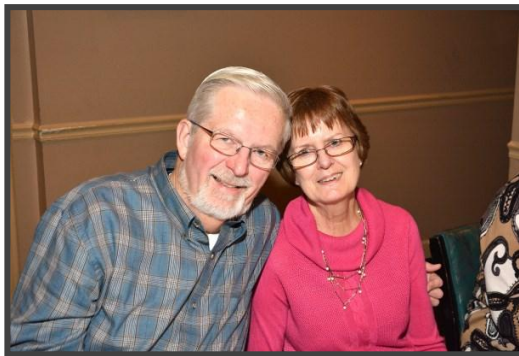
Blue Makes White

You may have read last month that three researchers received the 2014 Nobel Prize in physics for their invention of a blue LED. They were Isamu Akasaki, Hiroshi Amano, and Shuji Nakamura. The blue LED was important because it was the missing link needed to create white LED lighting. The white light from the sun can be reproduced artificially by blending three colours of light: red, green, and blue. LEDs are very efficient at converting electrical energy into visible light, but blue LEDs proved much harder to engineer than red and green ones. It took more than a quarter century after red LEDs were invented in the early 1960's before semiconductor materials and fabrication techniques grew sophisticated enough to enable blue LEDs in the mid-1990's. Gallium nitride was the key ingredient used by the Nobel laureates in their groundbreaking blue LEDs. Growing big enough crystals of this compound was the stumbling block that stopped many other researchers, but Profs Akasaki and Amano, working at Nagoya University in Japan, managed to grow them in 1986 on a specially designed scaffold made partly from sapphire. The key advantage of their invention is the production of white light with far less waste of electrical energy than with preceding technologies like incandescent and fluorescent lights. A quarter of world energy consumption goes to illumination.

These articles are from *Westlakes Amateur Radio Club Newsletter November & December 2014*

Pictures 2014 Christmas Party
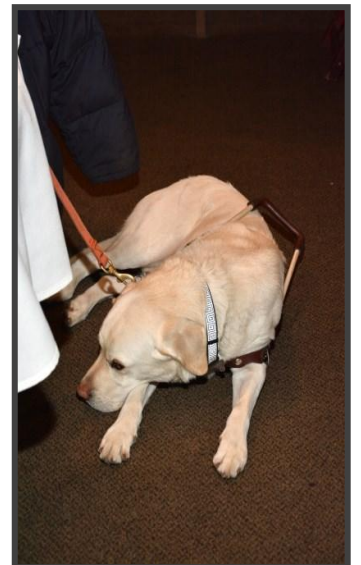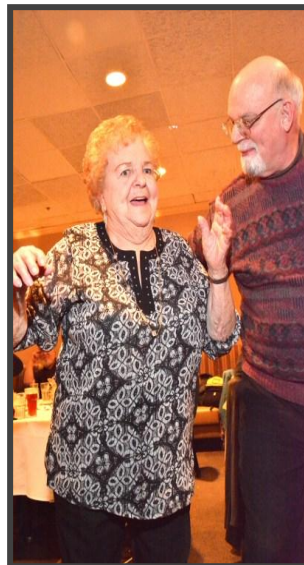
Happy New Year!

Hamfesters Amateur Radio Club

PO Box 474

Crestwood, IL 60445-0474

www.Hamfesters.org

Hamfesters Radio Club

Meetings and VE Testing

Club meetings are held on the first Friday of every month at the Crestwood Civic Center, 14025 Kostner Ave. in Crestwood, IL. Meetings begin at 7:30 PM. September meetings may vary if our meeting date conflicts with the Crestwood Flower show. Board Meetings: 7:30 PM on the 4th Monday of each month at the Crestwood Civic Center VE TESTING: Every 2nd Saturday of the Month at the Oak Forest City Hall, 15440 S. Central Ave. Testing begins at 9:00 AM but we ask that you arrive 10 minutes early. Exam fee is now $15.00. Al N9ZD VE Team Chairman

Special Activities

Hamfesters Big Peotone Hamfest: Our 79th annual Hamfest coming August 3, 2014-Will County Fairgrounds, Peotone, IL. Kerry AA9SB Hamfest Chairman.
Field Day: Join the W9AA crew for one of the best Field Days ever on June 28 & June 29 2014 at 115th and Oketo Avenue, Worth, IL. Jim KB9CYL Field Day Chairman
WAHM: Worked all Hamfester Members- work 10 Current members for a beautiful award certificate. Matt KC9JXC Awards

Nets/Contact Info

10 METER NET: Every Sunday Evening at 8:00 PM on 28.410. Bob W9TOE is Net Control

2 METER NET: Every Monday Evening at 9:00 PM on 146.640. Tom KA9ZXN is Net Control

W9AA Mailbox:145.650 24 hours a day. Bruno K9QKB is Sysop. ILOAK:Node on 145.650

WEB SITE: www.hamfesters.org Webmaster Granville, W9PNG &Brian ,W9HLQ

Club's address:
Hamfesters Radio Club
P.O. Box 474 Crestwood, IL 60445
Patti KC9LYE Secretary

Deadline for Submitting to the Hamgab is the fifteenth of the month.