ROUNDTABLE

The Denver Radio Club Newsletter

November 2011 Since 1917

PRESIDENT'S MESSAGE

By Bryan Steinberg – KB0A

As I write this month's column the snow is falling outside and the view has changed from fall to winter. The weathercasters' promise that we will get back to fall weather after this storm passes. So, for those who have procrastinated on getting their outside antenna work done this will serve as a warning. It's not too late to get ready for the real winter.

Speaking of getting ready, now is a good time with the HF bands showing more promise after the long (too long) hiatus of the solar minimum. Remember that even those holding Technician class licenses can get on the air using the HF frequencies. While CW is great for low power contacts, the digital modes are more popular than ever and there are many inexpensive ways to get started using them.

Thanks to Doug, N4ATA, for providing the October meeting presentation on Quick Response or QR Codes. You will find a recap of that meeting in this issue of the RoundTable. Also, a thanks to Bob, KC0CZ, for covering a much requested Elmer session topic on using EchoLink and the club's phone patch.

The club is looking for a new Education chairman. Bill, WA3H, who graciously took over the position when Rob, K0RAR, moved out of town, is unable to continue in that role. The primary job of the Education chair is to make sure that we have a presentation each month at the club's Elmer session. They don't need to present at every session but need to make sure that a presentation is made.

I would also like this person to attend as many of the weekly tech nets (Wednesday evenings at 7:30, except club meeting nights) and represent the club education activities. If you are interested, or would like to nominate someone who you feel would be good at this assignment, please contact me.

Thanks to Gerry, W0GV, for arranging for the continued use of the El Jebel site as our meeting venue through 2012. Remember to mark your calendar for the annual club holiday meeting; this will be in place of our regular meeting in December on the 21st. Once again we will be at the Country Buffet restaurant on Wadsworth in Littleton. More details in the December newsletter and on our web page.

I look forward to seeing all of you at the next meeting on November 16th at the El Jebel Shrine Center one block west of the intersection of 50th Avenue and Tennyson Street. Proceed to the second floor in the East Room. Please remember to always check our web site at http://www.w0tx.org for important information about the DRC. The Elmer Session and Tech Meeting begin at 6:30 pm immediately followed by the regular program at 7:30 pm.

Until next month…

Bryan – KB0A
President

INSIDE THE ROUND TABLE

NOVEMBER MEETING - WHAT'D I MISS

By Bryan – KB0A

The October meeting presentation was given by Doug, N4ATA, and detailed the history, use and creation of Quick Response Code, or QR Code. These square format tags are being found everywhere and are usually scanned using a smartphone. However, Doug told us that you can use any computer with a camera to scan them as well.

Doug explained the formatting of the QR Code and where specific information is contained in the tag which is used by the scanner to interpret the contents. The QR Codes are one form of 2 dimensional codes. Other 2D codes are bar codes, Microsoft Tags and Bee Tags. QR Codes can contain any type of data but is limited to about 4,000 alphanumeric characters. What the computer or phone does with the data depends on how the application which is used to scan the tag and how it is set up. In some cases the information is displayed on the screen, in other cases the smartphone can go directly to a coded website or call a phone number. So, you need to be careful what you scan and how your computer or phone handles the data.

More information on QR and other 2D codes can be found on Wikipedia, or one of the links Doug gave in his presentation:

- BeQRious — http://beqrious.com/generator
- I-nigma — http://www.i-nigma.com/CreatBarcodes.html
- QR Code Generator — http://invx.com
- Microsoft Tag — http://tag.microsoft.com/aspx
- Kaywa QR Code — http://qrcode.kaywa.com

Above are a some of QR Code tags you can try now. *Oh yeah, they don't have to be black!*

TECHNICAL COMMITTEE REPORT

By Bill – W6OAV

This report provides an overview of the items discussed during the October Technical Committee meeting. Items in black were agenda items. Blue are remarks to the agenda items.

Voter System

Goal: Design, build and test a 147.33 MHz voter system consisting of a central voter site and one remote site (Phase 1):

- Review the Phase 1 installation project:
  - ♦ Items not completed:
    - ◊ Check Station 4 UHF link receive antenna - KB0A will use his analyzer to verify the receive antenna system parameters.
    - ◊ Synchronize Station 4 and voter site 1hang times - KB0A will reprogram the voter site 1 radio to reduce the cross-band repeater hang time. He will also increase the power output level, if possible.
    - ◊ Calibrate the local and remote audio levels and responses - KB0A will use the IFR to set levels.
  - ♦ Status: No progress on these items
- Discuss Phase 2 possibilities:
  - ♦ K0RCW will run Splat, an application that profiles a transmitter's coverage areas, to determine Station 4's dead zones. The Tech Committee will then look for possible remote receiver sites in these zones.
  - ♦ Data on the repeater sites, except Squaw Mountain, has been sent to K0RCW. He will work on this as his time permits. He will do Station 4 and voter site 1 first.

ST. Anthony Repeater

Goal: Improve coverage:

- The present antenna will be replaced with the X30 omni vertical.
- WW0LF will make up a coax jumper for the new antenna.
- K0HTX will supply the necessary ladder when the antenna is replaced.
- Tech committee members will record the present signal strength for benchmarking after the antenna is replaced.
- Status: Need to find out height of the elevator tower. KB0A will call engineer at St. Anthony for info.

(Continued on page 3)

(Continued from page 2)

Noise at Station 4

Goal: Reduce the power line noise affecting all systems:

- W0WLF will get Xcel to generate a work order to resolve the noise issue.
- Status: No update as W0WLF was not at the meeting.

TS-940 Failure

Goal: Determine if re-soldering and cleaning connectors will fix radio:

- K0TOR has re-soldered many bad connections and replaced several bad solid state devices. He is now troubleshooting the built in automatic tuner.
- Status: Still working on TS-940 as time permits.

New MotoTRBO Repeater

Goal: Build a new MotoTRBO repeater:

- It was agreed not to replace the 448.625 repeater with the MotoTRBO. A number of club members use this UHF radio to access the club net on Sunday nights.
- Due to notification that digital repeater frequencies are going fast, Bryan has submitted a Request for Coordination (RSE) to the CCARC for a pair of MotoTRBO frequencies to be used by the club. The RSE has specified the St. Anthony Hospital campus as the site.

Additional Items

- W0GV is working to acquire a door key for the Hudson site.
- W0GV is working with the Rocky Mountain Ham group to keep status of their 3GHz data backbone system available to the Tech Committee.
- WW0LF is looking at feasibility of using a surplus Harris Marine HF radio for the 20 Meter side of the club packet gateway. Radio is 100W and designed for 100% duty cycle.
- Need to check and adjust, if necessary, the 448.625 repeater transmitted PL tone level. The level may be too low since a number of members state that the Tone Squelch on their radios will drop in the middle of a transmission when using this repeater.
- WG0N and K0HTX went to Squaw several weeks ago to check out the equipment and antennas. All looked good for the winter.

Upgrade 448.625 Repeater

Goal: Replace S Com 7k with S Com 7330 and write a program for the 7330.

- This project has been rescheduled for next spring.

SAFE WI-FI COMPUTING – PART 2

By Bill – W6OAV

Part 2 of this document discusses configuring and monitoring a home Wi-Fi network for best security. The reader might want to review the acronym definitions contained in the introduction to this document.

Home network encryption

We've all heard that we **must** configure security encryption on our home Wi-Fi network. What can happen if one uses no, or weak, Wi-Fi security? Many of those people have had to defend their innocence when accused by the feds of downloading child porn. Many have been robbed of their life savings. Many have had their identity stolen. The list goes on. The following described the three most common security encryption algorithms in ascending order of "robustness":

WEP

A weak encryption protocol which should not be used:

- Uses a single static always repeating encryption key between all network devices.
- Due to the static key, can be cracked in 3 minutes with readily available applications.
- Security tip - If you have equipment that cannot use any of the following encryptions, you should often change the WEP key (which is why routers generally allow storing up to four keys). The key must be changed at the same time in all devices on the network.

WPA

A much more secure encryption protocol:

- Uses a dynamically changing encryption key.
- Encryption key is different in every packet.
- Encryption key is different in each device.
- Can create up to 500 trillion combinations.
- Extremely difficult for hackers to read messages.
- Can be cracked in about 19 minutes with readily available applications.

WPA2

The most secure encryption protocol:

- Uses the AES (Advanced Encryption Standard) algorithm to encrypt data.
- Said to be theoretically un-crack-able due to the greater degree of randomness in the encryption keys that it generates.

(Continued on page 4)

(Continued from page 3)

Configuring a Home Wi-Fi Network

The following configuration steps will provide a relatively secure home Wi-Fi network:

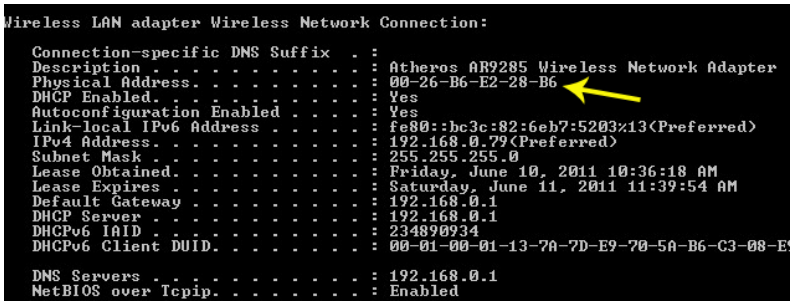
1. **Change the AP's default administrator password and SSID.** Hackers know all the default parameters if the defaults are retained. For example, if the SSID is Linksys, and the administrator defaults haven't been changed, the hacker now knows how to hack the AP and the network stations.
2. **Enable WPA2, WPA or WEP encryption** in that order. Use robust passwords containing lower case and upper case alphas, numbers and special characters such as "#". Never use such things as names, addresses, dates or plain text phrases.
3. **Enable AP's MAC Address Filtering.** This allows the AP to allow network access only to those stations in its wireless MAC Address Filter List. (This effects the Wi-Fi Authentication setup process described in Part 1 of this document). Consult your router's documentation for enabling MAC Address Filtering.
   Security alert – Not full proof as hackers using hacker software programs can easily fake (spoof) MAC addresses.
4. **Disable AP SSID Broadcast.** This hides the network from a casual "passersby's".
   Security alert - Hackers can use a Broadcast Probe to cause an AP to return a Probe Response as described in Part 1 of this document.
5. **Disable "Ad-Hoc".** This prevents hackers from "piggybacking" into one of the stations. This feature will be discussed in Parts 3 and 4 of this document. For tutorials, Google "Disable Ad-Hoc".
6. **Program a static IP address network.** This prevents the AP from allowing unauthorized stations access to the network. (Effects the Wi-Fi Association setup described in Part 1 of this document). The process is:
   - Disable the AP's DHCP which prevents the AP from assigning IP addresses to stations.
   - Assign static IP addresses to the network stations. For tutorials, Google "Static IP Addresses XP" or "Static IP Addresses Windows 7" as appropriate.
   - Program the AP to only allow connections to those static IP addresses. Consult your router's manual for the procedure.

   Security alert - Not full proof as hackers using hacker software programs can easily fake (spoof) IP addresses.
7. **Enable firewalls** on each station and the AP.
8. **Install good antivirus, and anti-malware software.** Keep these and the operating system updated. Make sure that the protection software includes protection against Rootkits and Keyloggers. (See note 1).
9. **Position the AP** to keep coverage only within the area of interest.
10. **Power down the AP** during extended times of non-usage.

Monitoring your Wi-Fi network

As can been seen above, hackers can defeat many of the security measures. Therefore you should periodically monitor your Wi-Fi network:

1. Install AirSnare (http://home.comcast.net/~jay.deboer/airsnare/). This is a free application that will look for unexpected MAC addresses on your Wi-Fi network and will monitor DHCP requests. There also other intrusion detections applications that work well to protect a network.
2. Periodically open your router's wireless status page. Check for unauthorized MAC addresses. If you don't know the MAC addresses of the stations on your network, at each station go to the Command Prompt window by clicking the Start button and then typing "run". When the command window opens type "ipconfig/all". The MAC address for that station will display as the Physical Address.



3. If you have Windows 7, check for unauthorized stations on your network by performing the following steps:

   Step 1. Click on the Start button, and then click Control Panel, *Figure 2 on Page 5 should appear.*

   Step 2. Click "View network status and tasks". *(See Figure 2 at the top of Page 5.)*

   Step 3. Click the house as depicted in *Figure 3*. The stations logged onto the network display. *(See Figure 4 at the top of Page 5.)*

(Continued on page 5)

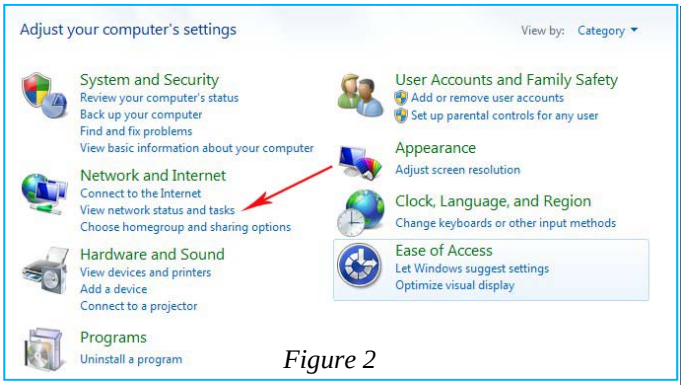


Figure 2

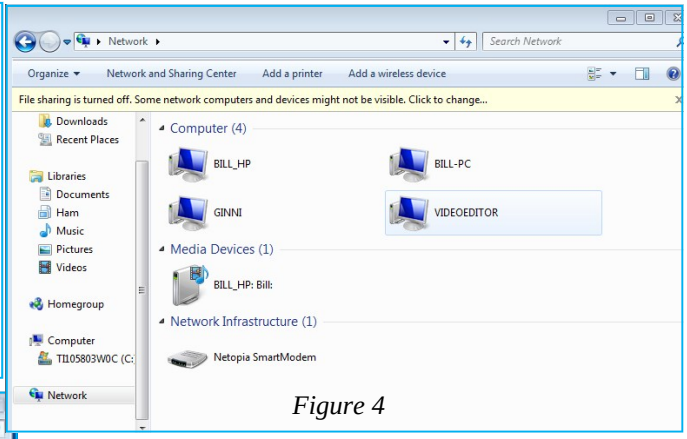


Figure 4

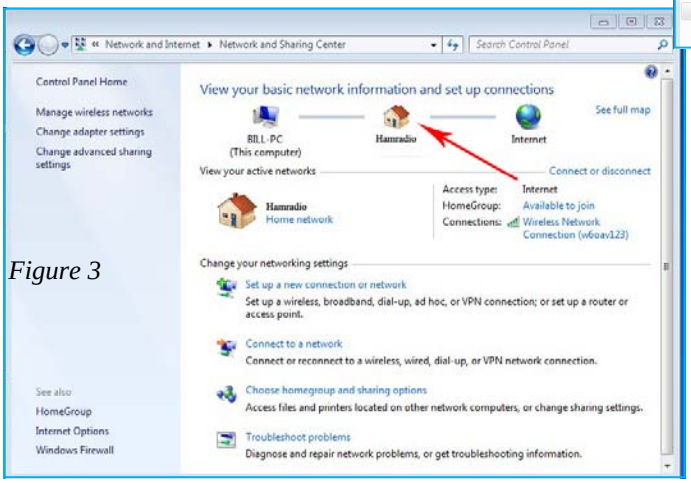
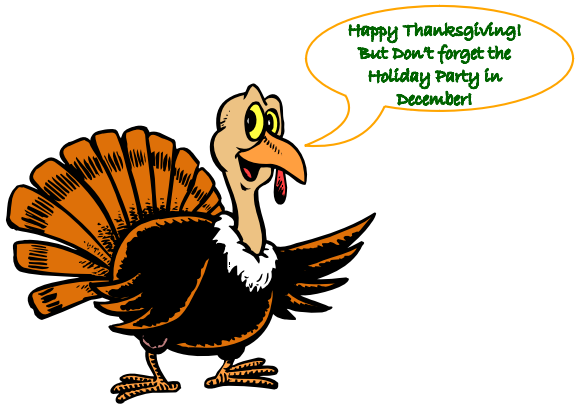


Figure 3

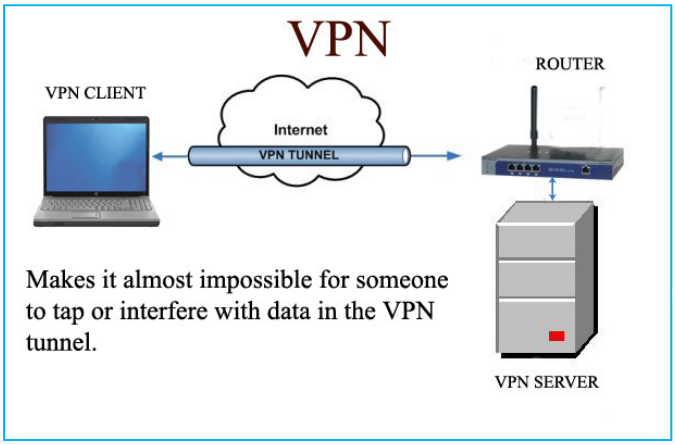


(Continued from page 4)

Keep in mind, the process is not "bullet proof". A knowledgeable hacker can make his station invisible on your network.

Be totally secure – use a Virtual Private Network (VPN)

There is only one virtually hacker proof configuration which keeps your sensitive data secure, assuming your station is not infected with Rootkit or a Keylogger (see note 1). The configuration uses a Virtual Private Network (VPN), illustrated below.



A VPN is a logical tunnel through the internet. The tunnel extends from the inside of the station to the inside of a VPN server. The data is encrypted before it enters into the Wi-Fi network and decrypted by the far end after it exits the internet. It is as if the remote station is on the same local network as the VPN server. VPNs almost make it impossible for hackers to tap into the data stream. More on this in Part 6 of this document.

Parts 3 and 4 of the document will discuss configuring Window 7 and Window XP computers for secure Wi-Fi hotspot operation. Never forget that a Wi-Fi hotspot is a "war zone" and a favorite "playground" for hackers.

Note 1:
Rootkits are malware applications that imbed themselves into the operating system and record keystrokes before they encrypted into any security applications. They also may give the hacker administrator privileges giving him complete control of the station. Rootkits can be installed when a hacker hacks a network or when a station user downloads an infected file or application from a hacker's Web site.

A Keylogger is a hidden program designed to record keystrokes. Some versions can also take screenshots. This information is then sent to the hacker.

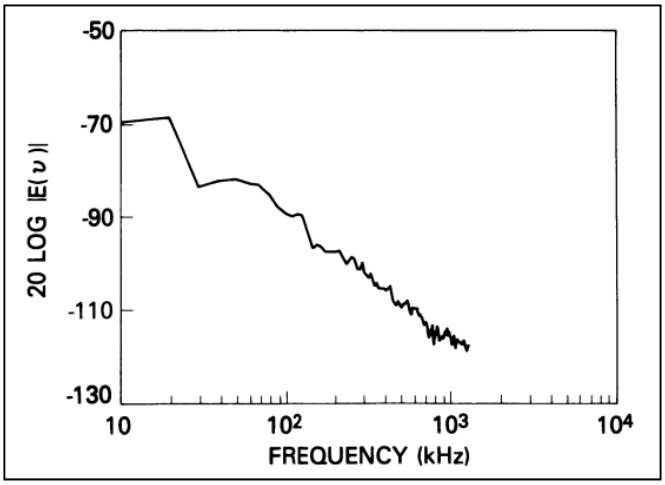
LIGHTNING DAMAGE — CAN IT BE STOPPED WITH A COIL?

By Bill Hester – N0LAJ

Following our recent DRC meeting presentation on lightning protection for ham radio, I have received several questions about commonly recommended methods to prevent lightning damage.

One of these questions asked if using an impedance matching coil, connected between the radiating element and ground at the base of a 160 meter band vertical antenna, could provide lightning protection. This question arose from a technical article in which the author stated: "The inductor also works as a static bleed choke and will definitely help save equipment if the antenna has a lightning hit or nearby hit. This is a pretty elegant solution for a matching device, a static bleed choke, and a surge arrestor all in one single component!" (1)

If lightning consisted only of a simple direct current flow, this technique might work.



However, since lightning discharge waveforms show significant energy extending from D.C. up to around 5 MHz (2), and if the inductance of the matching coil presents significant impedance for these frequencies, then there can be a rather high voltage differential created across the coil and the coax connection. The effective capacitance from the antenna to ground may help to reduce the higher frequency voltages, but there will certainly be an impedance peak, with a corresponding lightning induced voltage peak, at the matching system's resonant frequency when the antenna system is tuned for operation below 5 MHz

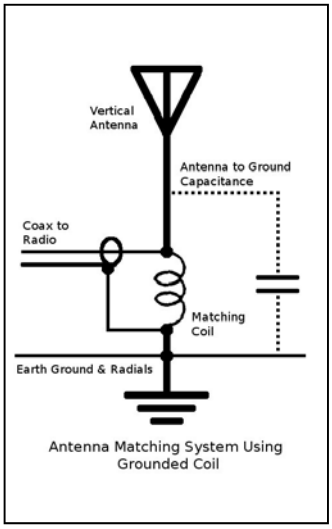
To "ballpark" the possible magnitude of the induced voltage, we can first calculate the impedance presented at the coax connection by the matching coil and the antenna capacitance/radiation resistance combination.

Then we can take that value and "force" a lightning strike current of 5,000 amps (3) through that impedance to get the resulting differential voltage produced across the coax feedpoint. This is a valid analysis method because lightning acts as a constant-current-generator energy source while discharging the cloud-to-earth charge differential.

As an easy, simplified, example, if the impedance at the antenna's resonant frequency is 50 ohms resistive (at a resonance frequency below 5 MHz), then using ohms law: *Voltage = Current x Impedance (in simple form) = (5,000 amps x 50 ohms) = 250,000 volts.*

A voltage of this magnitude is high enough to cause arcing to ground at the base of the antenna. Typical coax dielectric insulation will puncture through, and there will be a high voltage surge-wave moving down the coax toward the radio equipment. This is why the use of a single-point-ground bar (the SPG, as discussed in the meeting presentation), located outside the building, equipped with good quality Polyphaser type sacrificial surge arrestors, and a very good, low-impedance, grounding system, is still needed to minimize the surge voltage hitting the radio.

For antennas tuned for the higher frequency bands (well above 5 MHz), the available lightning discharge energy will fall mostly below the antenna's resonance point. This, along with the lower matching coil impedance used with higher frequency antennas, will result in lower induced voltage. I doubt however, that the resulting voltage will be low enough to completely avoid radio equipment damage.



Antenna Matching System Using Grounded Coil

In summary, my opinion is that a matching coil *(illustrated at right)* will bleed off D.C. static build-up (4), but it is not a surge arrestor, and it doesn't really provide adequate lightning protection by itself.

References and notes:

(1) "Tuning a 160M Full Sized Vertical with Strong AM Broadcast RF Present on the Antenna", by Jay Terleski, WX0B.
http://arraysolutions.com/images/Tuning_160m_Vertical.pdf
(2) NASA Technical Memorandum 87788, "Review of Measurements of the RF Spectrum of Radiation from Lightning".
(3) This is the projected lightning strike current at 5 MHz, as produced by an average 50,000 amp lightning strike. This is determined from the negative slope of lightning energy vs. frequency as shown in the accompanying graph. The slope is -20 dB per decade.
(4) Static build up is caused by wind flowing across the antenna.

OPERATION MOUNTAIN GUARD

BY BOB – KB0BZZ

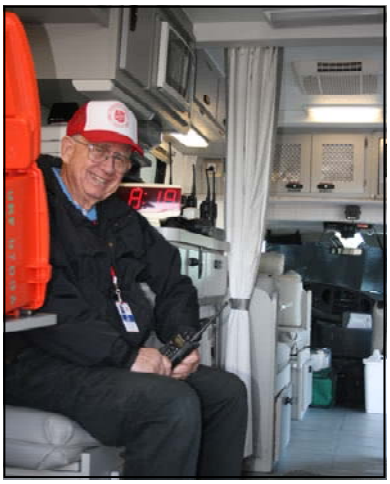
On September 23rd, the North Central Region All-Hazards group held a Metro-wide terrorist attack exercise. There were four separate attack scenes running concurrently. The intent was to stress local responders with multiple concurrent incidents. Over 100 agencies participated representing the Federal, State, County and local levels.

Several DRC members participated with our served agency, The Salvation Army (TSA). They ran 4 Nets and provided communications support to TSA management, Logistics, and on-site mobile kitchens.

DRC members that participated were Jim Beal (K0TOR), John Bridges (N0QOP), Joel Zachrich (N0KEX), Jennifer Suggs (KD0KSS), Jack McComb (W0JMC), Chris Tenorio (KD0DUJ), Lance Wilson (N1RTV), Jack Dowd (N0QHF), and Jerome Davidson (N0OMA).

The Salvation Army expressed their sincere "Thank You" to the DRC members that helped make this exercise a success!

Bob Zimprich
DRC Emergency Communications Chairman



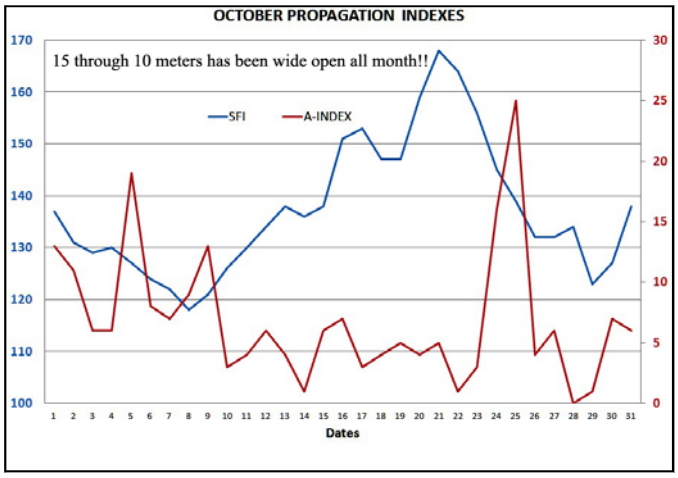
PAST & FUTURE PROPAGATION CONDITIONS

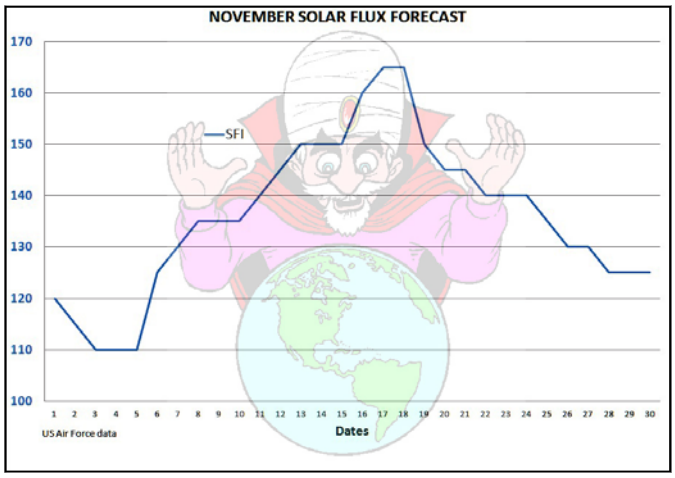
By Bill – W6OAV

This article provides two charts: the propagation conditions for last month and a forecast of next month's propagation conditions.

USING THE PROPAGATION INDEX CHART

Note two things on the chart: the trend of the SFI and A indexes and the date of largest SFI peak. The trend of the SFI shows the progress of the solar cycle during the past month. The SFI peak allows the rough forecasting of the reoccurrence of SFI peak in the next month. In order to "forecast" the next SFI peak, note the date when the SFI peak occurred and project out to about 28 days. Due to the sun's 28 day rotation, the SFI peak will often reoccur in about 28 days. The reason is because the sun spots causing the SFI peak move with the sun's rotation and face the earth every 28 days. This 28 day repetition will become more pronounced as the solar cycle improves. Refer to the September 2010 *Roundtable* for more complete information on the "SFI" and "A" indexes.





NOVEMBER MEETING ANNOUNCEMENT

Digital Radio — Legal On Ham Bands!

ANALOG HAS ITS LIMITS: Digital opens up a world of possibilities including clearer audio, integrated voice and data on one device, applications such as text messaging, GPS location tracking, telephony, dispatch, 40 % longer battery life, and more…

MotoTRBO uses TDMA technology and is narrowband, allowing for two channels within the narrowband specification of 12.5 kHz!

Come hear Steve Cohan talk about MotoTRBO at the next meeting.

MOTOROLA

As you noticed, it is getting 'COLD' out there.
So, stay warm and support the DRC with a new DRC Logo Jacket.

The jackets are Black with Grey fleece lining and are embellished with Your Name & Call Sign on the left chest and the DRC logo centered on the back.

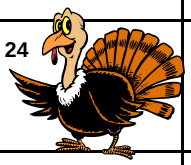
Still just $60.00 plus applicable taxes through December 2011

Call or email Doug (N4ATA) with your Name, Call Sign and size of jacket size. Phone: (303) 922-3305 (8am-5pm, M–F)

Contact: jtbembsvcinc@comcast.net or N4ATA@comcast.net (*Please, put DRC Jacket in subject line*)

NOVEMBER 2010

DRC Net Sunday 8:30pm Local

Sunday	Monday	Tuesday	Wednesday	Thursday	Friday	Saturday
		1	2 *Learning Net* 7:30pm First Quarter	3	4	5 *ARRL* November *CW* Sweepstakes Begins 2100U
6 Mountain Standard Time Begins 	7 *ARRL* November *CW* Sweepstakes Ends 0259U	8	9 *Learning Net* 7:30pm	10 *Veteran's Day*  Full Moon	11	12
13	14	15	16 *DRC Meeting* Elmer 6:30pm General 7:30pm	17	18 Last Quarter	19 *ARRL* Nov. *Phone* Sweepstakes Begins 2100U *ARRL* EME Contest Begins 0000U
20 *ARRL* EME Contest Ends 2359U	21 *ARRL* Nov. *Phone* Sweepstakes Ends 0300U	22	23 *Learning Net* 7:30pm	24 	25 New Moon	26
27	28	29	30			

Check www.ARRL.org for Contests and Rules!

DRC Board of Directors

President	KB0A	Bryan Steinberg	303-987-9596	KB0A@arrl.net
Vice-President	W0GV	Gerry Villhauer	303-467-0223	W0GV@arrl.net
Secretary	WW0LF	Orlen Wolf	303-279-6264	owolf@mines.edu
Treasurer	K0TOR	Jim Beall	303-798-2351	K0TOR@arrl.net
Board Member	WG0N	Dave Baysinger	303-987-0246	WG0N@arrl.net
Board Member	K0HTX	Dave Gillespie	303-880-1938	K0HTX@comcast.net
Board Member	KD0CXX	Paul Meenach	720-746-1488	TBD
Board Member	N3PQ	Frank Ortega	303-452-0283	N3PQ@hotmail.com

DRC Staff and Volunteers

Trustee	WW0LF	Orlen Wolf	303-279-6264	owolf@mines.edu
Net Control	K0TOR	Jim Beall	303-798-2351	K0TOR@arrl.net
Emergency Coordinator	KB0BZZ	Bob Zimprich	303-400-3400	bobzz@comcast.net
Membership	KC0CZ	Bob Wilson	303-659-0517	KC0CZ@comcast.net
Club Librarian	WG0N	Dave Baysinger	303-987-0246	WG0N@arrl.net
VE Team	K0RCW	Robert White	303-619-1048	K0RCW@arrl.net
Swapfest Mgr	KB0A	Bryan Steinberg	303-987-9596	drcfest@comcast.net
Field Day	K0HTX	Dave Gillespie	303-880-1938	K0HTX@comcast.net
Tech. Committee Chair	W6OAV	Bill Rinker	303-741-2537	W6OAV@arrl.net
APRS Chair	KB0MQQ	Lloyd Plush	303-277-0785	LloydPlush@aol.com
Benevolent		Carolyn Wolf	303-330-0721	
RT Editor	AG0S	George McCray	303-751-7246	AG0S@arrl.net
Education	OPEN			
Salvation Army Liaison	KB0BZZ	Bob Zimprich	303-400-3400	bobzz@comcast.net

DRC Repeaters

BAND	Freq / Shift / PL Tone	Additional Information
6m	53.090mHz (-1mHz)	
Packet	145.05mHz<>14.105mHz	
2m	145.490mHz (-) 100Hz PL	**Linked to the 70cm - 448.625mHz machine.**
2m	147.330mHz (-) 100Hz PL	**Local Area, Members Auto-Patch Does Not TX a PL!**
2m	147.330mHz (-) 131.8Hz PL	**NE Area Remote Does Not TX a PL!**
1.25m	224.380mHz (-) 100Hz PL	
70cm	448.625mHz (-) 100Hz PL	**Linked to the 2m - 145.490mHz machine.**
70cm	449.350mHz (-) 100Hz PL	**Wide area coverage with Echolink Node # 4140.**

Editor's Note

DRC members - this is your newsletter. If there is something which is club or amateur radio related that you'd like to see as a regular feature, email suggestions to the editor. Members are the heart and sole of The Denver Radio Club, if you have an expertise or an interest in a particular segment of ham radio that you'd like to write about, you may email your submissions to AG0S@arrl.net. Submission deadline is the 25th of the Month. **Editor**