JUG

Publication of the Northern California Contest Club

NCCC

Issue 485

October 2012

Inside this issue:

Guests are always welcome at the NCCC!
Please join us.

Next Meeting

"WPX for is for Lovers" -Andy Faber AE6Y

Date:
Monday 8th October.

Time:
6:00pm schmooze, 6:30pm dinner
7:00pm program

Location:
Faultine Brewing Company

Address:
1235 Oakmead Parkway Sunnyvale, CA 94085

http://www.faultlinebrewing.com/

From the President…

Summer is officially over and we're into the Fall and the contest season. I hope you are savoring the pleasantly warm days and counting down the days to the California QSO Party… just a short week away!

For the CQP "Green" team, this is crunch time as final PR messages go out, final club presentations get made and the software folks are keeping their fingers crossed that everything will work (smoothly!).

Here's a heads-up… The Worldwide Radio Operators Foundation (WWROF) has taken over the sponsorship of the Webinar program established by our friendly rivals at PVRC. John K6MM will be participating in a webinar this coming Monday October 1st at 6pm PDT – "A look at the upcoming PA and CA QSO Parties" – you can find a signup at https://www2.gotomeeting.com/register/925057098 (free of charge) for a last minute insight into these two contests.

Propagation wise, things are looking up with flex levels getting higher and 10m showing more than a few signs of life! When you operate 10m during CQP, remember you will find many new hams, especially technician class holders who are new to HF and newer still to contesting. Although we all savor high rates, remember that contests are also teaching moments and an opportunity to recruit more folks to radio sport. So take a few moments and guide a newbie through the exchange – and smile – we all had those moments on the other end years ago.

Better still, if you have a new ham as a friend and you aren't personally out to break a record (or two), give them some BIC time and use CQP as a mentoring event.

Speaking of propagation, if you would like to generate your own propagation predictions tailored to your own station configuration, check out http://k6tu.net - this is a web service for generating predictions and is available at no charge to NCCC members who have paid their current year's dues.

KB, have FUN and see you on the air!

Stu K6TU

Officers:

President	Stu Phillips	K6TU	stu@ridgelift.com
Vice President	Dean Wood	N6DE	cqden6de@gmail.com
Secretary/Treasurer	Dave Ritchie	W6DR	nccc.treasurer@gmail.com
Past President	Chris Tate	N6WM	ctate@ewnetinc.com
Director	Kevin Rowett	K6TD	kevin@rowett.org
Director	John Miller	K6MM	k6mm@arrl.net
Director	Ira Stoler	K2RD	k2rd@arrl.net

Volunteers:

New Member Mentor	Al Rendon	WT6K	wt6k@arrl.net
Charter Member	Rusty Epps	W6OAT	w6oat@sbcglobal.net
Awards Chairs	Joanna Dilley	K6YL	joanna.k6yl@gmail.com
	Rebar Rebarchik	N6DB	rebar@hamilton.com
CQP Chair	Alan Eshleman	K6SRZ	doctore@well.com
CQP Certificates	Andy Faber	AE6Y	ae6y@arrl.net
K6ZM QSL Manager	George Daughters	K6GT	k6gt@arrl.net
K6CQP,N6CQP,W6CQP QSL Mgr	Ed Muns	W0YK	w0yk@arrl.net
NCCC Email reflector Admin	Phil Verinsky	W6PK	kb-w6tqg@verinsky.com
Webmaster	John Miller	K6MM	k6mm@arrl.net
JUG Editors	Ian Parker	W6TCP	w6tcpian@gmail.com
	Stu Phillips	K6TU	stu@ridgelift.com

Thursday Night Contesting:

NCCC—Sprint	Ken Keeler	N6RO	kenkeeler@jazznut.com
NS Ladder	Bill Haddon	N6ZFO	haddon.bill@gmail.com
Slow NS (SNS)	Chris Tate	N6WM	ctate@ewnetinc.com

NCCC Net

Thursday 8 PM

Freq: 3.610 +/-

NCCC

Monthly meetings take place on the second Monday of each month !

Details here

NCCC Membership Information

If you wish to join NCCC, you must fill out an application for membership, which will be read and voted upon at the next monthly meeting. (PDF application form)

To join, you must reside within club territory which is defined as the maximum of:

- Northern California, anything north of the Tehachapi's up to the Oregon border, and
- A part of north-western Nevada (anything within our ARRL 175-mile radius circle centered at 10 miles North of Auburn on Highway 49).

NCJ NA CW Sprint Recognition

The September 2012 CW Sprint results are in. Congratulations to NCCC members for another tremendous performance!

- NCCC #1 won the team competition. It's the first time we have won a September CW Sprint since 2006.
- NCCC #1 had 128,339 points, and the next closest team was the Dallas Fort Worth Contest Group #1 at 117,195 points. This is a substantial margin in any CW Sprint.
- NCCC member Trey N5KO won the entire contest. It's been an extremely impressive summer for Trey, as he also won NAQP CW in August.
- NCCC was the only club to submit 3 teams.
- 15 of our 22 team members scored more than 10,000 points, with all 10 on NCCC #1 reaching that milestone.

Thanks to Bob W6RGG for organizing our NCCC teams. I'd also like to recognize all of the NCCC participants in the CW Sprint who joined an NCCC team:

- **NCCC #1:** N5KO (@W6NL), N6RO, K6XX, N6XI, W6YX (N7MH op), AE6Y, K6AW (@N6DZ), K9YC, AJ6V, K6SRZ
- **NCCC #2:** K7GK (@W6JZH), W6RGG, N3ZZ, N6ZFO, KZ2V (@W6CS), KA3DRR (@W6SL), W6SX, W6CT, K6CSL
- **NCCC #3:** K6VVA, NQ6N, W6NF

Upcoming Calendar:

California QSO Party: October 6 16Z – October 7 22Z
http://cqp.org/Rules.html

NA Sprint RTTY: October 14 0Z – 4Z
http://ncjweb.com/sprintrules.php

CQWW DX SSB: October 27 0Z – October 28 24Z
http://cqww.com/rules.php

VP/CC Report
Dean Wood, N6DE

Tom W6IXP SK

It is with great sadness to report the passing of Tom W6IXP, who become a silent key today. He went way to fast and he will be missed greatly by his large family, his friends, and the ham radio community.

Native Village Kids shown Left to Right
Isacc, (Bossy not shown), Moses, Franklyn, and Jared.
Tom, W6IXP operating at the mic headset.

Left to Right: Tom W6IXP, Pat Omiak IRA President
Native Village of Diomede, and Barry K6ST
(Photograph by Dwayne Ahkvaluk,)

Tom was a member of the NCCC (Northern California Contest Club) and enjoyed ham radio contesting from his hilltop qth in Grass Valley. He loved attending at the Visalia DXconvention, especially hanging out at the hospitality suites, swapping stories and brain storming ideas on ham radio. Prior to Grass Valley, Tom use to live in the greater Half Moon Bay area in Montara when I first met him on the Coastside in 1995.

In 1996 Tom and I attended the Visalia DXconvention where we heard a presentation on IOTA (Island on the air) and several months later, we went on our first IOTA expedition to Santa Cruz Island IOTA NA-144 off the coast of Venture (southern California). Next Tom did a IOTA expedition to Alaska NA-157 Kayak Island. In 1998 Tom and I put on the most wanted North America IOTA NA -150 Little Diomede Island in the Bering Straights of Alaska just a couple of miles from Russia. On the same expedition we activated Sledge Island IOTA NA-210 a new never been activated island. In 2000, we went back to Alaska to activate two new never been activated IOTAs: NA-214 Stuart Island and NA-215 Chamisso Island. See http://www.barrybettman.com/na150/

In the past few years, Tom shifted some of his interests from ham radio to autocross car racing. Tom was an explorer and software chip engineer. He had an amazing attitude, an amazing family, and an amazing life. Please help me honor Tom W6IXP.

73,
Barry K6ST

California QSO Party

CQP & improving your operating skills

Quick! Mark the weekend of October 6th and 7th on your calendar and start planning for a weekend of radio fun! The first full weekend of October marks the annual running of the California QSO Party (CQP) – the most fun you can have with a radio if you live in the Golden State! This year marks the 46th running of CQP sponsored by the Northern California Contest Club.

Why contest? From an operating point of view, most aspects of Ham Radio from Public Service, chasing DX to working contests have one thing in common – accurate and timely copying of information often under stress.

Entering a contest either casually to give some points or as a serious effort, is a great exercise in operating "under fire".

The first full weekend of October (October 6th & 7th this year) sees the annual running of the California QSO Party – a great opportunity for stations in California because everyone else HAS TO WORK US!

We are the DX!

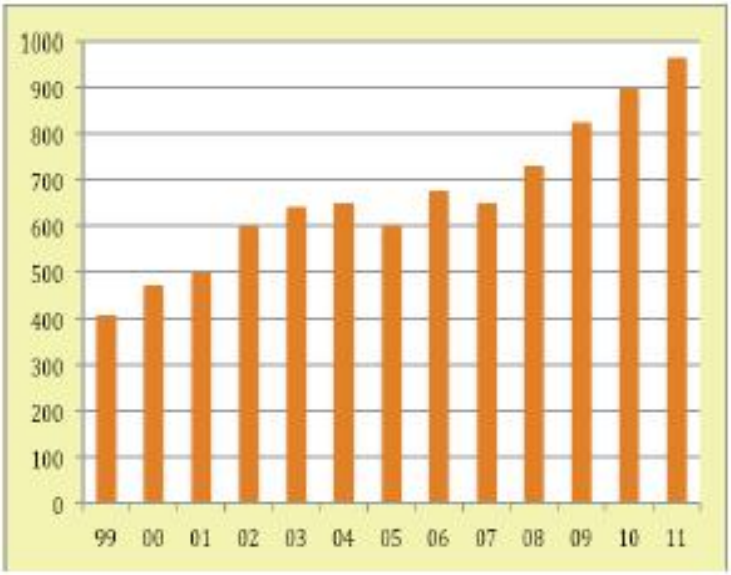
Whether you're a "Big gun" or "Little pistol", CQP is a great opportunity for you to be on the receiving end of a pileup or to search and pounce for other states and countries. You can easily Work All States in a single weekend especially with everyone looking for you. And there's DX to be worked: it's possible to work all continents during CQP.

For California stations the object of the contest is to work as many stations as possible on SSB and CW. You can work the same station on each band and each mode for score credit. Every US state and Canadian province you work counts as a multiplier – 58 total for us just like the number of counties in California.

Want to be on the end of a really big pile up? Plan a County Expedition to one of the rarer California counties--the rest of the world will beat a path to You. Check out the counties activation planning map on the CQP web site at www.cqp.org - you may be surprised that some of the rarest counties often lie on your doorstep.

Low Power, High Power? CW or SSB? CQP is a fun contest for all.

CQP is sponsored by the Northern California Contest Club, and led by a group of dedicated, experienced team members. NCCC volunteers help with PR, planning county expeditions and processing all the logs to score the contest.



CQP continues to see healthy growth in submitted logs. In 2011 we had almost 1000 logs submitted! CQP rivals many national and international contests in participation and awards. Our goal is to break the 1000 log level in 2012.

Every station that submits a log is eligible for an achievement certificate and there are several operating categories where the leader receives a special CQP plaque for proud display on the shack wall. Of course, since we are in California, the top 20 scores submitted in California and Outside California qualify for a special award – a bottle of NCCC Private Reserve Wine with personalized label. The wine is graciously donated by Twisted Oak Winery and is a limited production Tempranillo crafted by wine maker and NCCC member Jeff Stai, WK6I.

Three categories are designed to encourage operation in contests:

- YL award
- Youth (< 18) award
- California New Contester

So if you've never entered a contest or have only dabbled in the past, this award category is for you!

If you work all 58 counties, you qualify for the "Worked All California Counties Award" sponsored by NCCC.

You can find the full rules and award details on the CQP web site at http://www.cqp.org.

Part time or full, home operator or an expedition to a new county, CQP is a blast!

We hope you will join us this year and have a lot of Fun!

Stu Phillips – K6TU, NCCC President
Alan Eshleman, K6SRZ, CQP CHair

Publication of the Northern California Contest Club

Technical Topics

SAFE WIFI COMPUTING

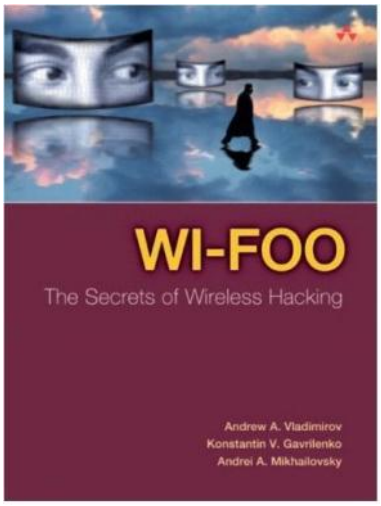
By Bill, W6OAV

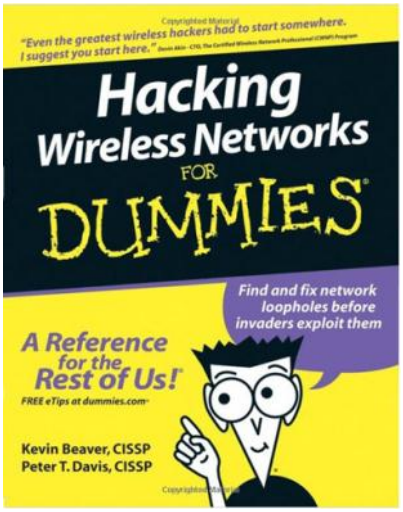
Introduction

After I finished my "Safe Wi-Fi Computing" talk at our club meeting {Denver Radio Club) a few months ago, several attendees asked if I would document the talk. So…here goes.

Using Wi-Fi, both at home and in Wi-Fi hotspots (hotels, airports, coffee shops, etc.), is a way of life these days. Unfortunately, Wi-Fi exposes users to identity theft and capture/control of the user's computer. There is only one way to completely protect one's self. This document provides information which will help the reader to understand how Wi-Fi systems work, how to configure/ monitor home Wi-Fi systems and how to operate securely over both home and hotspot Wi-Fi systems.

So, why worry about Wi-Fi security? Well, not only does the Internet contain a wealth of Wi-Fi hacking information, there are many books out on this subject.





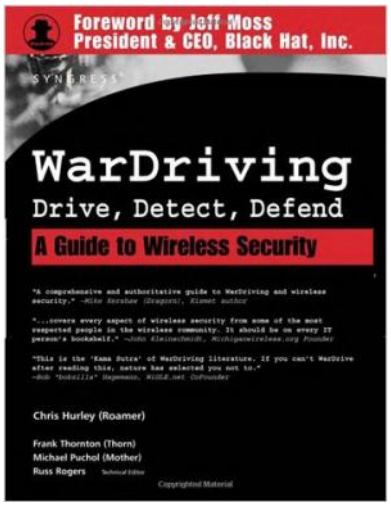


Figure 1. Hacking is so prevalent there is even a "Hacking for Dummies" publication! Figure 2. Stop in Barns and you will find a monthly hacker's magazine called *2600*. Then, there is War Driving. Figure 3.

So, what is War Driving? War Driving is a hacker activity where hackers drive around with very sophisticated hacking applications and high gain antennas that can detect Wi-Fi networks up to 25 miles distance. These hackers not only look for unsecured Wi-Fi networks but most also have the ability to hack into secured Wi-Fi networks as well. Then, there are the War Driving clubs where members gather to brag about how many secured Wi-Fi networks they had hacked!

To give an idea of how ramped Wi-Fi hacking is becoming, consider this. According to several computer magazines, a free hacking application called Firesheep has been downloaded over a million times. Think the down loaders are doing this for fun?

This 6 part document will cover the following topics:

Part 1 – How Wi-Fi systems and security measures function.

Part 2 – Configuring and monitoring home Wi-Fi networks for best security.

Continued on page 4

Part 3 – User guide for configuring Win7 for secure operation in Wi-Fi hotspots.

Part 4 – User guide for configuring WinXP for secure operation in Wi-Fi hotspots.

Part 5 – Various ways hotspot hackers can attack your computer.

Part 6 – Defeating hackers with the only secure Wi-Fi configuration.

Definitions

Before we start, we need to define a few acronyms which will appear throughout this document. Make sure you understand them or keep this part of this publication handy as you read the upcoming parts.

Wi-Fi – A local area network that uses high frequency radio signals to transmit and receive data over distances of a few hundred feet. Uses Ethernet protocol.

SSID – The name of the Wi-Fi network.

AP – An access point (AP), usually a router, controls access between the Internet and Wi-Fi equipped stations (laptops, computer towers iPads, etc.)

Station – A Wi-Fi equipped device (laptop, iPad, iPhone, etc.) that normally communicates with an AP.

IP Address – A unique number which identifies an AP or a station and its location on the network

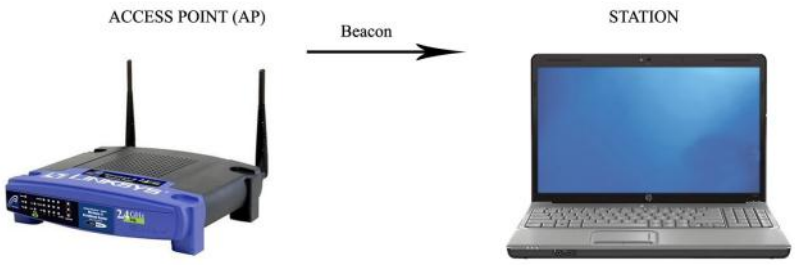
SAFE WIFI COMPUTING – PART 1

By Bill, W6OAV

Part 1 of this document describes how Wi-Fi works. Why understand how Wi-Fi works? Understanding how Wi-Fi works will make it easier to understand why and how to configure Wi-Fi systems and how to operate safely, especially in Wi-Fi hotspots (hotels, airports, coffee shops etc.). Wi-Fi hotspots must be considered as war zones where operating is very dangerous, as will be discussed later in this document.

A high level overview of Wi-Fi setup process

The discussion below is a high level overview of the Wi-Fi setup process. It is based on a station using standard Windows Wi-Fi drivers. If 3rd party Wi-Fi drivers are used there may be some small variation in the process described below. Before continuing, the reader might want to review the acronym definitions contained in the introduction to this document.



IDLE WI-FI - AP BEACONS

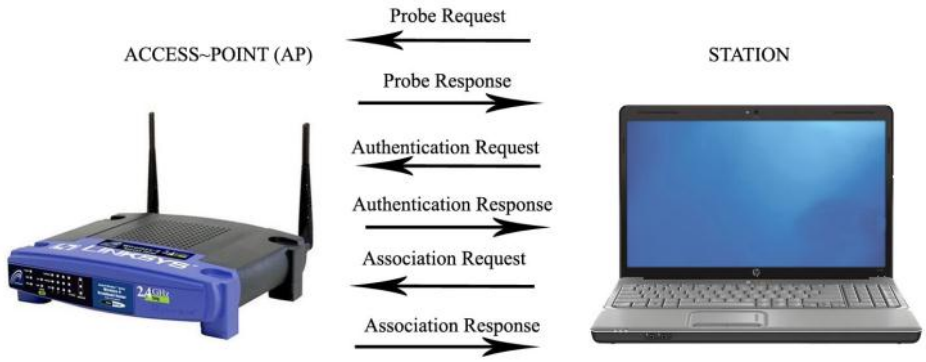
AP Beacons

Definition: A *beacon* is a Wi-Fi management data frame which an Access Point (AP), usually a router, transmits to announce its presence.

An AP normally transmits a beacon every 100 ms. The beacon contains the AP's MAC address, SSID, and other communications process information.

A Wi-Fi equipped station, upon hearing a beacon (or beacons if more than one AP in range is beaconing), will add the SSID(s) to its "Available Networks" list. The station will then respond either manually or automatically with a Probe Request as discussed below.

Probe Requests and Probe Responses



Definition: *Probe Requests* and *Probe Responses* are used by a station and an AP to exchange communication parameters.

A station transmits a Probe Request to an AP when that station wishes access to the AP's network. The Probe Request contains the AP's SSID and the station's SSID and the station's communication capabilities.

How a station transmits a Probe Request depends upon whether it is configured for manual or automatic connects:

A station, configured for ***manual connects***, will display on its Wi-Fi screen the newly heard beacon SSID(s) as "Available Networks". When the station user clicks the Connect Button for a particular SSID, the station will send out a Probe Request for that network.

A station, configured for ***automatic connects,*** and having one of the available networks in its Profile List from a past automatic connection, will automatically send out a Probe Request for that network. More on automatic connects later as this can be a dangerous security issue, especially in Wi-Fi hotspots. Hackers can use this feature to capture and control stations.

The AP responds with a Probe Response if it has been configured to allow that particular station network access. The Probe Response contains the AP's capabilities. **Security Note:** This is an important point where security measures can be implemented. More on this in Part 2 of this document.

Authentication Requests and Authentication Responses

Definition: *Authentication* is the process where the AP verifies and accepts or rejects a station's Probe Request.

The station responds to the AP's Probe Response with an Authentication Request listing the parameters it wishes to use based on its and the AP's capabilities. This includes speed, encryption (Open, WEP, WPA or WPA2) and the encryption key, if encryption is enabled.

If the station meets all the AP's requirements, the AP responds with an Authentication Response allowing the station to continue to the next step of the setup process. If the AP has been programmed to only allow certain station MAC addresses or SSIDs to gain network access, the AP will not authenticate the station. **Security Note**: A security feature called MAC Filtering can be implemented here. More on this in Part 2 of this document.

Association Requests and Association Responses

Definition: *Association* is the process where the AP and the station agree on the parameters to be used when the AP grants the station full access to its network.

The station now sends an Association Request confirming the parameters to be used.

The AP responds with the Association Response. The AP's DHCP assigns an IP address to the station and a gateway address to be used (usually that of the AP). Two way traffic can now begin **Security Note**: Security features called DHCP Disable and Static IP Addressing can be implemented here. More on this in Part 2 of this document.

Station's Beacon Process

In order to operate securely, one must understand the station's beaconing process. When the station's Wi-Fi is enabled it goes through two modes, the *active* scan mode and the *passive* scan mode:

Active scan mode - When the station's Wi-Fi is turned on it immediately begins to transmit Probe Requests on each Wi-Fi channel for each network contained in its Profile List. If an AP returns a Probe Response, the station, if configured for **manual** connects, displays the network(s) in its "Network Availability" list. If the station is configured for **automatic** connects, it begins the Wi-Fi automatic setup process described above. **Security Note:** This is an important area where security measures can be implemented. More on automatic connects later as this can be a dangerous security issue, especially in Wi-Fi hotspots. Hackers use this feature to capture and control stations.

Passive scan mode – If there are no responses in the active scan mode, the station scans each Wi-Fi channel listening for AP beacons. Any beacons heard will be displayed on the station's Wi-Fi screen as "Available Networks". The station user then can manually initiate a connection to one of the networks.

Beacon security tips

One often hears that on a home network the AP should be configured not to beacon. If it doesn't beacon, then neighbors and hackers won't know that it is present. This isn't true for hackers and certain station Wi-Fi applications.

Hackers can transmit Broadcast Probe Requests that will cause most non beaconing APs to return a Probe Response. Also, some stations will transmit a Broadcast Probe Request in the active scan mode that will cause an AP to respond with a Probe Response. Disabling AP broadcasts is a good idea but don't hang your hat on being protected when doing this.

Stations also continue active and passive scanning while connected to a network. The reason is for roaming. Should the station loose contact with a network, if configured for automatic connects, the station will establish a connection to another available network if that network is in the station's Profile List and set for automatic connects. Usually, the station user will not be aware of the switch. Hackers can take advantage of this issue as will be discussed later.

Part 2 of this document will discuss properly configuring and monitoring a home Wi-Fi network for maximum security

SAFE WIFI 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.

Configuring a Home Wi-Fi Network

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

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.

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.

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.

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.

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".

Program a static IP address network. This prevents the AP from allowing unauthorized stations access to the network. (Effects the Wi-Fi Association setup process 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.

Enable firewalls on each station and the AP.

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).

Position the AP to keep coverage only within the area of interest.

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:

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.

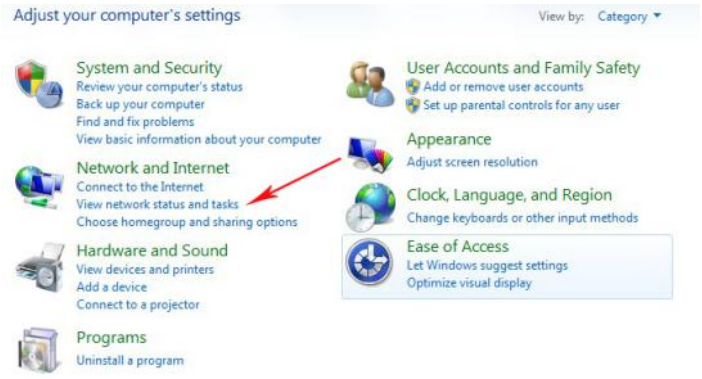
```
Wireless LAN adapter Wireless Network Connection:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Atheros AR9285 Wireless Network Adapter
   Physical Address. . . . . . . . . : 00-26-B6-E2-28-B6
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::bc3c:82:6eb7:5203%13(Preferred)
   IPv4 Address. . . . . . . . . . . : 192.168.0.79(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Lease Obtained. . . . . . . . . . : Friday, June 10, 2011 10:36:18 AM
   Lease Expires . . . . . . . . . . : Saturday, June 11, 2011 11:39:54 AM
   Default Gateway . . . . . . . . . : 192.168.0.1
   DHCP Server . . . . . . . . . . . : 192.168.0.1
   DHCPv6 IAID . . . . . . . . . . . : 234890934
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-13-7A-7D-E9-70-5A-B6-C3-08-E

   DNS Servers . . . . . . . . . . . : 192.168.0.1
   NetBIOS over Tcpip. . . . . . . . : Enabled
```

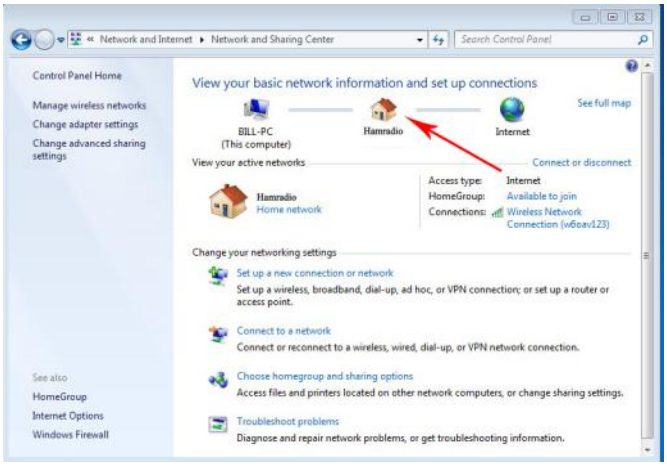
Periodically open your router’s wireless status page. Check for unauthorized MAC addresses. If you don’t know the MAC addresses of the stations on your network, at each station go to the Command Prompt window by clicking the Start button and then typing “run”.

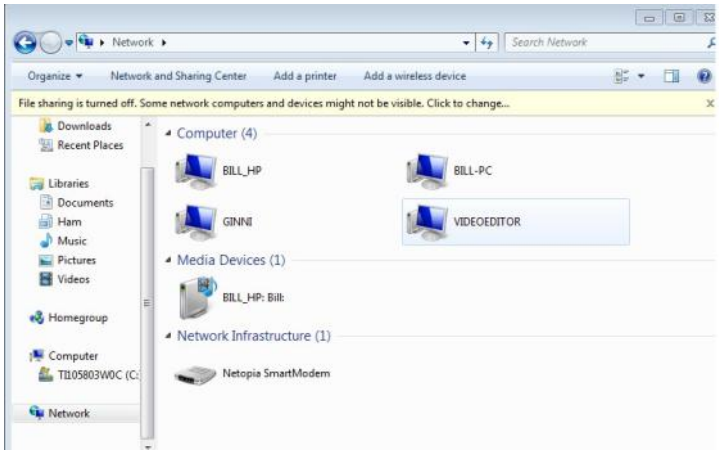
When the command window opens type “ipconfig/all”. The MAC address for that station will display as the Physical Address. Figure 1.



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. The screen below appears.



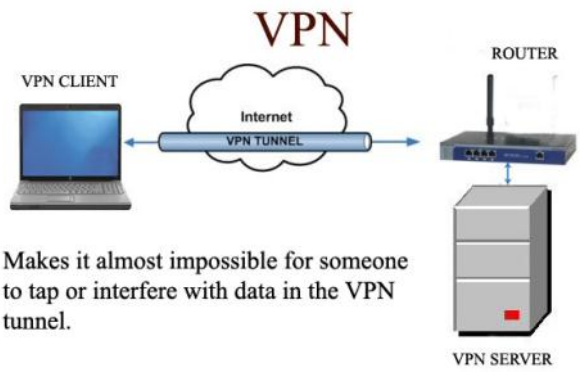


Step 2. Click “View network status and tasks”.

Step 3. Click the house. The stations logged onto the network display.

Keep in mind that this 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).

.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 “play ground” 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.

SAFE WIFI COMPUTING – PART 3

By Bill, W6OAV

HOTSPOT SECURITY

As mentioned earlier is this document, Wi-Fi hotspots are considered “war zones” where the enemy is hackers waiting to attack a user’s station. Part 3 of this document discusses configuring a Windows 7 station for secure hotspot operation. Part 4 will discuss configuring a Windows XP station for secure hotspot operation. A lot of the following information also pertains to using these operating systems on home Wi-Fi network. Depending on how your computer is configured, your screens may be a bit different than those shown below. If so, the following will serve as a guide for configuring your system. The reader might want to review the acronym definitions contained in the introduction to this document.

Configuring and using Windows 7 in hotspots.

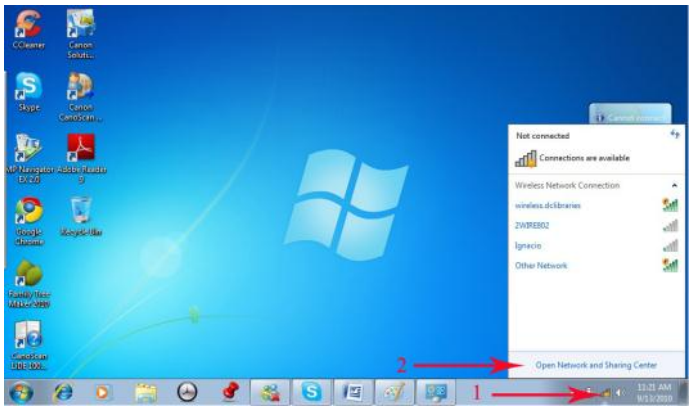
When a user begins the Wi-Fi connection process, Windows 7 gives the user a choice of using a private or a public profile. The private profile is for use on a private Wi-Fi network and the public profile is for use on a hotspot Wi-Fi network. Using a public profile automatically tightens up the firewall security settings.

Before enabling the station’s Wi-Fi for hotspot use, the user needs to insure that the options are set in the public profile which disables file sharing and makes the station invisible to other stations on the hotspot Wi-Fi network. This aids in preventing hackers from attacking the station.

Also, the user must disable Automatic Connects to all but the home network contained in the station’s Wi-Fi Profile List. Disabling Auto Connects prevents the station from automatically connecting to a bogus hotspot network. For example, a hacker at a hotspot may be emulating an AP and beaconing as several common networks, such as Starbucks, Barns and Noble, Free Wi-Fi, etc. Should one of these networks be in the station’s Profile List, and set for Auto Connects, the station may connect to the bogus network. The user may not be aware of the bogus connection. Also, even if the station user connects to a valid hotspot Wi-Fi network, a hacker can force the station to disconnect and reconnect to his bogus network if Automatic Connects has not been disabled. This feature, called Roaming, was discussed in Part 1 of this document. Roaming allows a station to automatically connect to another network if contact is lost with the original network.

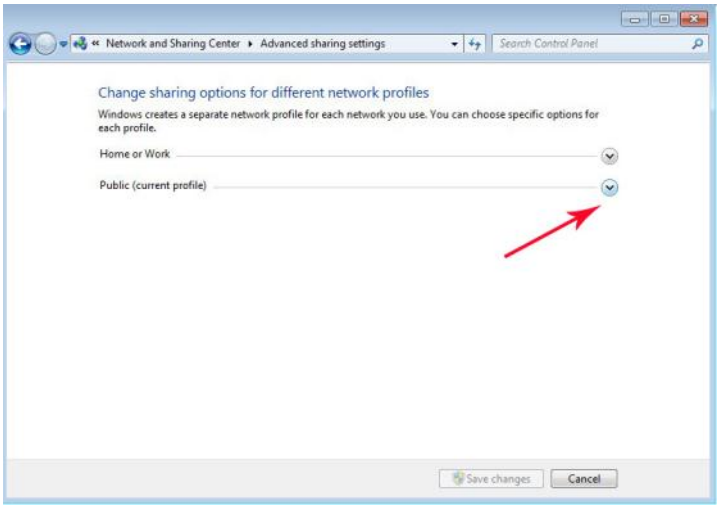
Disabling File Sharing and making the station invisible.

To configure the public profile to disable file sharing and to make the station invisible to other hotspot stations perform the steps below.

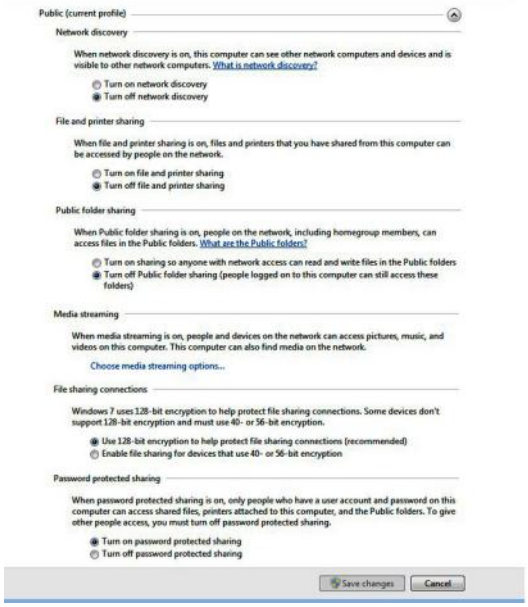


Step 1. On the desktop, click the Wi-Fi icon and then click “Open Network and Sharing Center”.

Step 2. Click on “Change Advanced Sharing Settings”.



Step 3. Click the “Public Profile” drop down button.



Step 4. Click the profile items as shown below and click “Save”

The following describes the parameters that are disabled when configured as shown.

Network Discovery – OFF

This parameter prevents the station from connecting to other stations (ad-hoc) and allowing the station only to connect to an AP.

File and Printer Sharing – Off

This parameter prevents users on the internet from accessing these files.

Public File Sharing – OFF

This parameter prevents users on the internet from accessing these files.

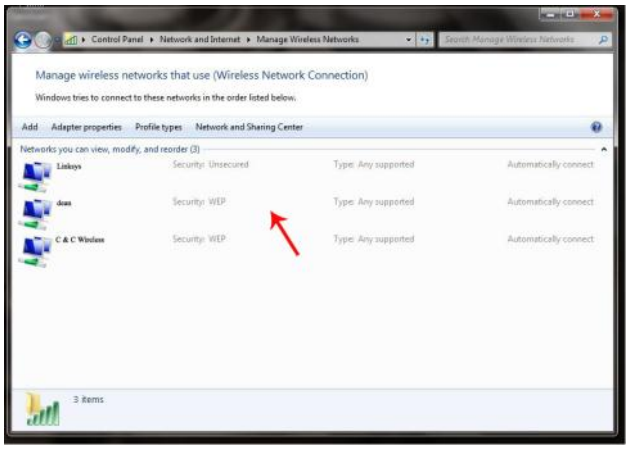
Password Protected Sharing – OFF

Prevents other users from accessing shared files.

Disabling Auto Connects

To access the Wi-Fi Profile List and disable the Auto Connects, perform the steps below.

The following screen appeared when the “Save” button was clicked in Step 4 above.



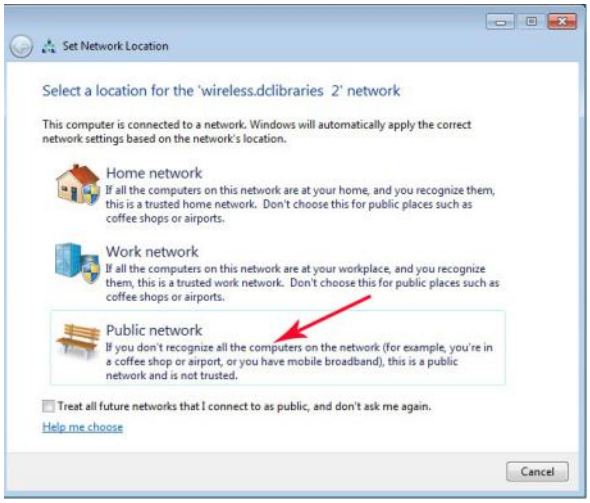
Step 1. Click on “Manage Wireless Networks” to access the station’s Profile List..

Step 2. To disable the Auto Connect option on a network, click the desired network (In this example “dean”).

Step 3. Deselect “Connect automatically when this network is in range”. Click ”OK”. Repeat steps 2 and 3 for any other network set for auto connect (except for “trusted networks” such as your home network).

Step 4. Go back to the desktop and enable the station's Wi-Fi. Click the Wi-Fi icon and then click the "Connect" button for the desired network shown in the "Available Networks" list. Do not tick the "Connect Automatically" box. Doing this will re-enable the network in the Wi-Fi Profile List for auto connects.

Security tip – Before connecting to a hotspot Wi-Fi, verify the SSID with the Wi-Fi provider to insure that you are connecting to a valid network. For example, airports and most coffee shops will normally display their network SSID.



Step 5. Click "Public Network". This not only increases Firewall security settings but also activates the settings chosen earlier. Windows 7 will then connect to the network.

Part 4 of this document will discuss configuring a Windows XP station for secure hotspot operation.

SAFE WIFI COMPUTING – PART 4
By Bill, W6OAV

Part 4 discusses and illustrates configuring Windows XP for secure hotspot Wi-Fi operation. A lot of the following also pertains to configuring Windows XP on home Wi-Fi systems. The reader might want to review the acronym definitions contained in the introduction to this document.

Preparing For Hotspot Wi-Fi Operation

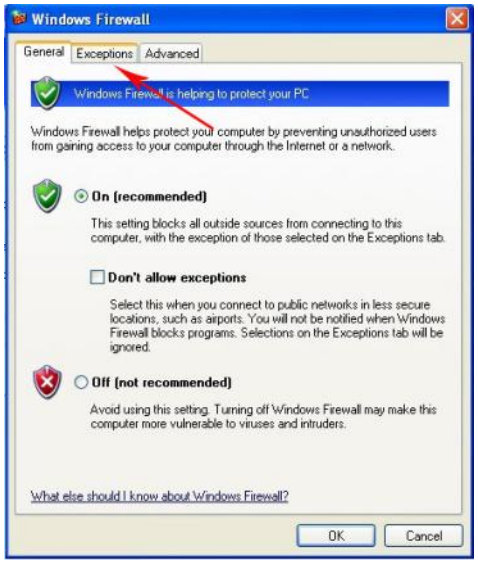
For secure hotspot operation, the user must disable file sharing options, Ad Hoc connections and automatic connects to networks, other than the home network, contained in the station's Wi-Fi Profile List.

The station's Wi-Fi must be enabled in order to disable the above mentioned features. Therefore, it is best to perform these procedures in a safe place, such as at home or in a non-hotspot location. If these procedures must be done in a hotspot, verify the SSID of the Wi-Fi offered by the hotspot operator. Then, after enabling the station's Wi-Fi, verify that it hasn't connected to any Wi-Fi. If it has, and it is not that of the hotspot provider, immediate turn off the station's Wi-Fi. Then move to a non-hotspot location and disable the above mentioned features.

Technical Topics—continued

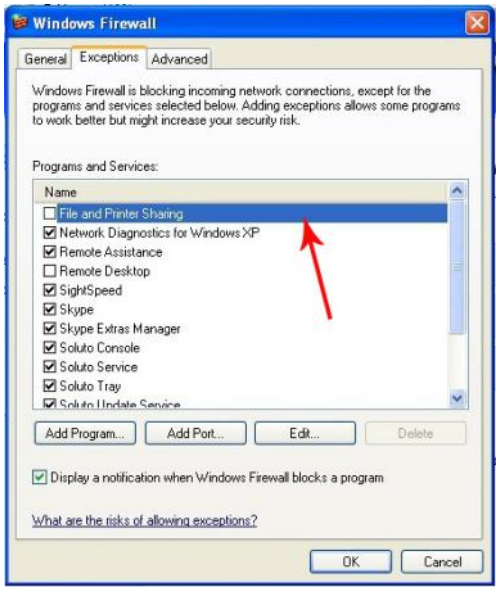
The figures shown below are for an XP configuration set for the classic view. As is normal for Windows there are several different ways to achieve the following configurations. If your configuration is set for a different XP configuration, or if you are using a 3rd party Wi-Fi application, your screens will be a bit different. However, the process is the same.

Disabling File Sharing options.



Step 1. Bring up the Security Center by clicking “Start”, “Settings”, “Control Panel” and then “Security Center”. On Windows Security Center click “Windows Firewall”.

Step 2. Click on Exceptions tab.

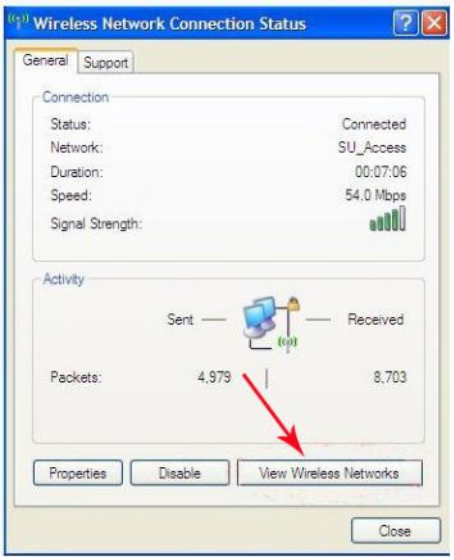


Step 3

Un-tick “File and printer sharing”. Click “OK” and close all windows which will bring up the Desk Top.

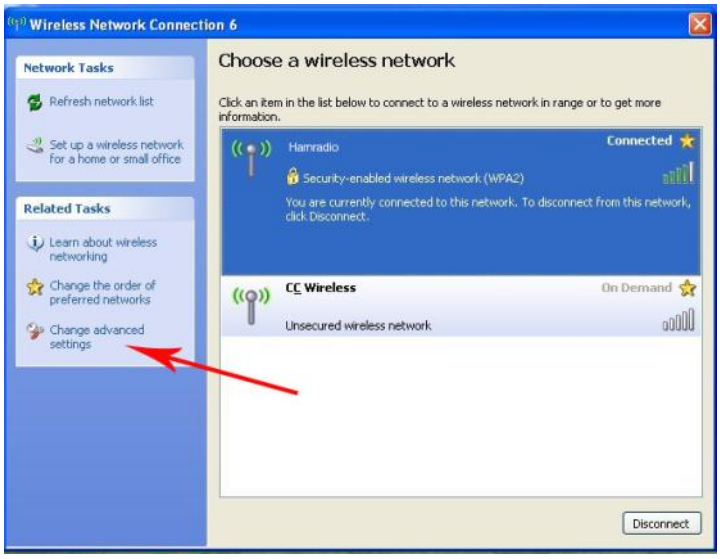
Disabling Ad-Hoc Connections

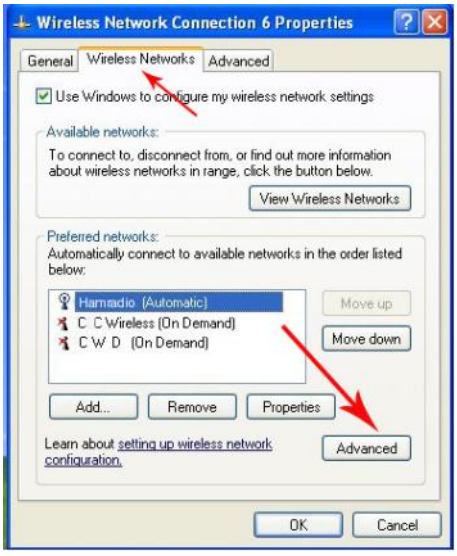
Turn on the station's Wi-Fi. Then perform the steps shown below:



Step 1. Click the Wi-Fi Icon in the System Tray.

Step 2. Click "View Wireless Networks".





Step 3. If you are in a Wi-Fi hotspot, check to see if your station is connected to a network which is not the network that you verified earlier with the hotspot operator. If not, immediately disconnect from that network. (Note that "Hamradio" is connected in this example). To get to the Wi-Fi Profile List, select any network ("Hamradio" in this example) and click "Change Advanced Settings".

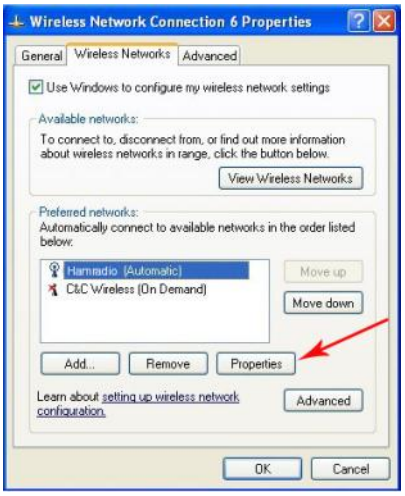
Step 4. Click the "Wireless Networks" tab and the click the "Advanced" button. This screen shows the Wi-Fi Profiles stored in the station. Note that the network "Hamradio" is configured for auto connects and that the other two networks are configured for manual connects.

Note that one can select an undesired Wi-Fi Profile and click “Remove” to delete it. To disable “Ad Hoc connections on a particular network, select the desired network and click “Advanced”.

Step 5. Click “Access port (infrastructure) networks only” & then click “Close”.

Step 6. Repeat the above steps for any other desired networks.

Disable Auto Connections



Step 1. Click the desired network and click the “Properties” button.

Step 2. If necessary, click the “Connection” tab. Un-Check “Connect when this network is in range” & then “OK”.

Step 3. Repeat the above steps for any other desired networks.

Part 5 of this document will discuss some of the common ways hackers can attack your station.

.SAFE WIFI COMPUTING – PART 5

By Bill, W6OAV

Part 5 discusses some of the common ways hackers can attack a station at a Wi-Fi hotspot. The reader might want to review the acronym definitions contained in the introduction to this document.

First a couple of questions:

If the hotspot is using WPA2, the most robust encryption, is a station user safe when using this network? The answer… Not necessarily. Everyone using the WPA2 network was given the same password. Hence, everyone is using the same encryption.

Are you safe when accessing a web site using https://www? ("https" means that the connection to the web site is encrypted). The answer…Not necessarily. Many sites encrypt the log-in but not the cookie that is transmitted after the log-in. A hacker can capture that cookie for hacking by using a free Firefox plug-in called Firesheep. Keep in mind that, according to several computer magazines, this plug-in has been downloaded over a million times! Do you think these people are downloading this application just for the fun of it?

There are many ways the hackers can attack your station and/or intercept your critical information. Some of the most common ways are described below.

COOKIE CAPTURE

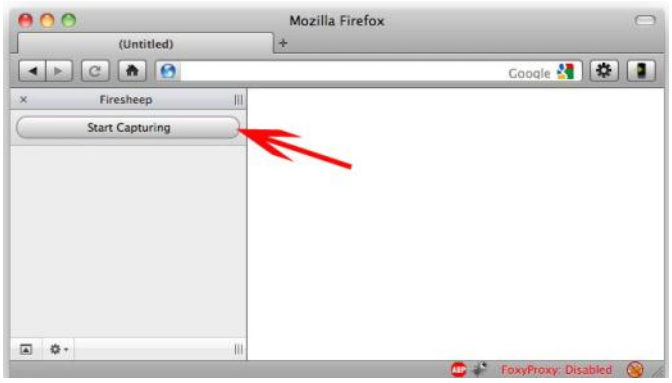


Figure 1

Figure 2

Figure 3

As described above, a hacker, using Firesheep, can capture un-encrypted cookies when station users log into web sites, even if the log-ins are encrypted (https://www). A hacker, after bringing up Firesheep, clicks the "Start Capturing" button to monitor all traffic. Figure 1. When Firesheep sees un-encrypted cookies, it captures and displays them. Figure 2. Now, the hacker can use one of the cookies to access that unsuspecting cookie owner's web site. For this discussion, assume that the hacker clicks Ian's Facebook icon. The hacker now becomes Ian on Facebook and can do anything that Ian can do. Figure 3

How does one combat Firesheep? Down load and install a free application called Blacksheep. As shown in Figure 4 Blacksheep detects and alerts the user that Firesheep is operating in the vicinity.

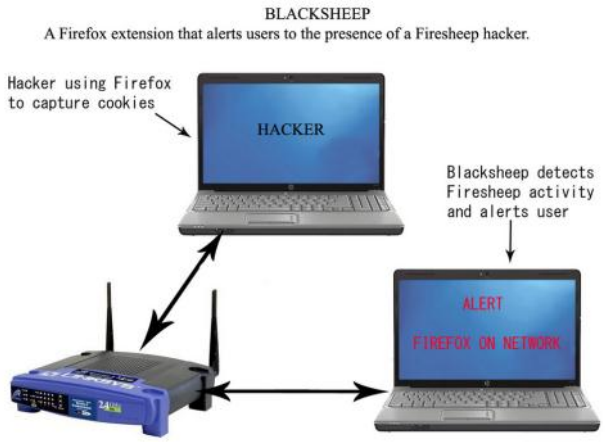


Figure 4

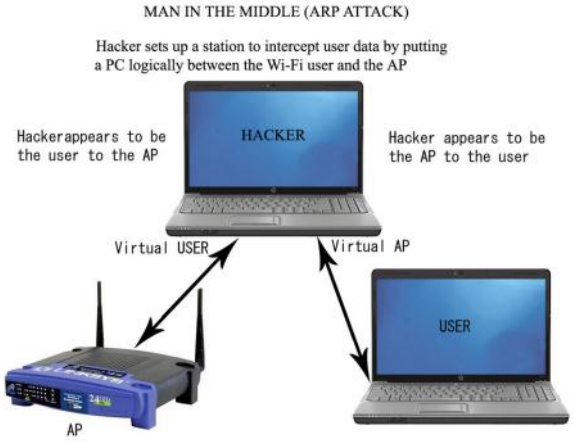
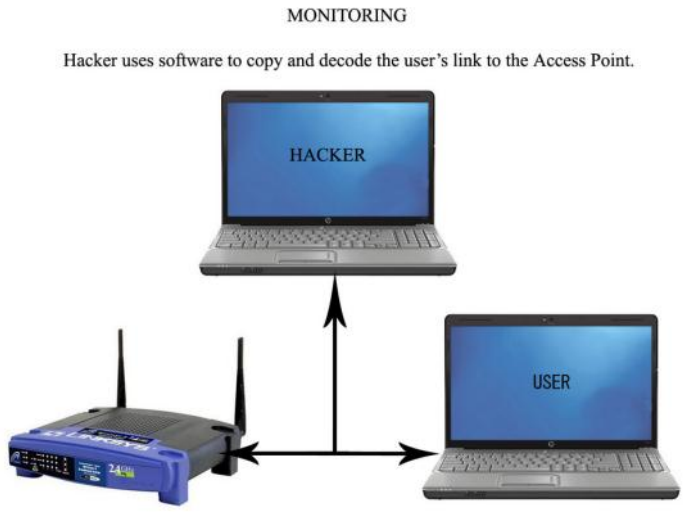


Figure 5

MAN IN THE MIDDLE

Another common hacker attack is called “Man in the Middle” which is also known as an “ARP Attack”. …The description of which is beyond the scope of this article. Referring to Figure 5 the hacker, using ARPing, becomes an AP to the station user and the hacker becomes the station user to the hotspot AP. Therefore, the hacker is logically between the user and the AP. The hacker can now intercept all traffic.



MONITORING

There are sophisticated applications that actually allow hackers to decode, monitor and record traffic between the user and the AP. Figure 6.

SHOULDER SURFING

An effective, and low tech method, used by hackers is over the shoulder surfing. The hacker basically stands behind the victim and observes the important key strokes. Sometimes the hacker will use a camcorder at a distance, zoom in on the user’s keyboard and record the keystrokes. Sometimes the hacker will sit near an unsuspecting user and use a Smartphone to video important keystrokes.

THE THUMB DRIVE

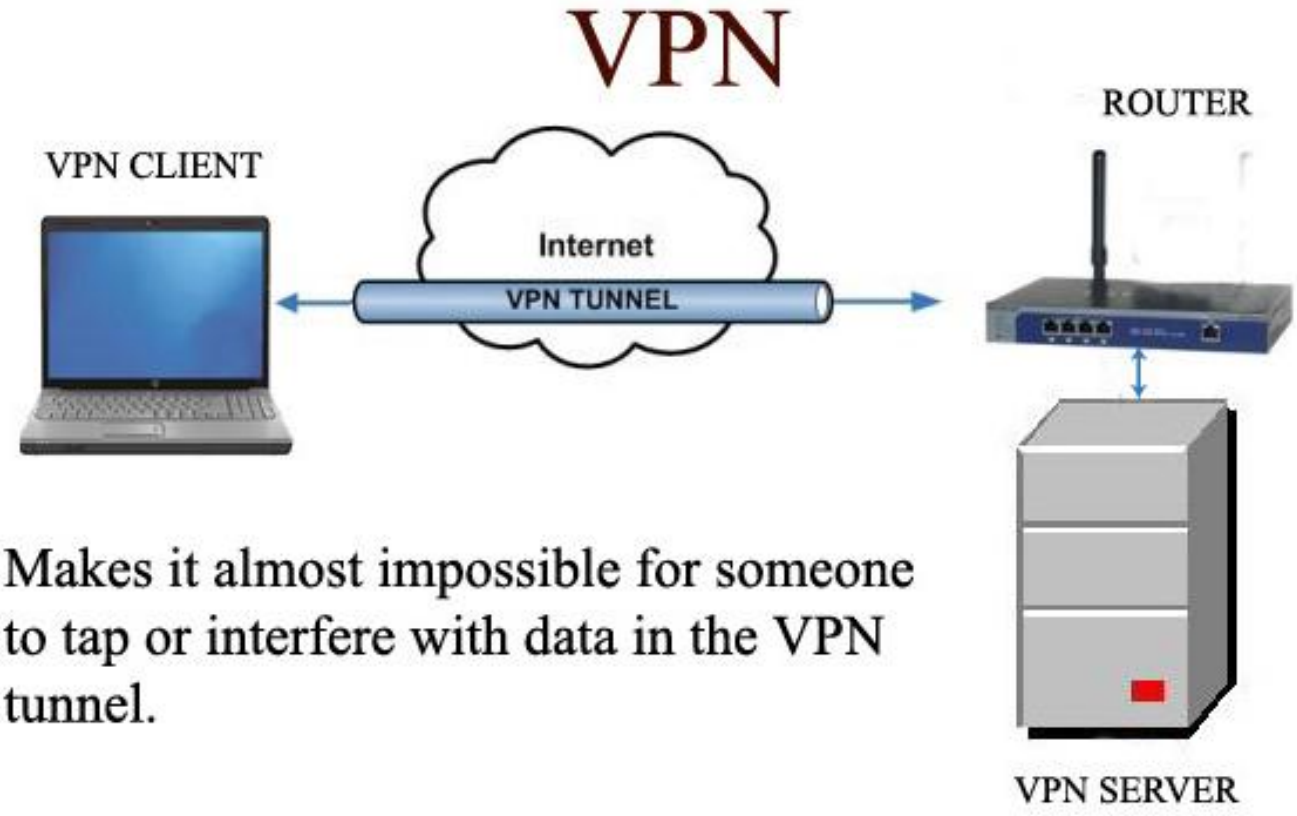
Hackers will sometimes leave a nice looking thumb drive lying in a hotspot location. The finder plugs the thumb drive into his station to see what is on it. He might find a few interesting innocent items on the thumb drive. However, unknown to the user the activation of the thumb drive loaded a keylogger or other malware onto the station.

Part 6 will discuss how to handle these security situations.

SAFE WIFI COMPUTING – PART 6
By Bill, W6OAV

Part 6 discusses and illustrates the only really secure way to operate on a home or hotspot Wi-Fi. Part 6 ends with overall conclusions.

VIRTUAL PRIVATE NETWORK (VPN)



There is only one virtually hacker free method. The method uses a VPN. Figure 1. A VPN is a highly encrypted logical channel, or tunnel, through the internet. The tunnel extends from the inside of the station to the inside of a VPN server. The station's data is encrypted before it is entered into the Wi-Fi network and decrypted once it arrives at the VPN server. The same is true from the VPN server to the station. 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.

There are free VPN services and fee based VPN services. The free VPN services are usually not as fast as the fee based VPN services and one must occasionally look at ads. Examples of free VPN services can be found at:

http:/hotspotshield.com

http://www.anchorfree.com

When relying on the security of a VPN, one must insure that the station does not have a Rootkit installed.

CONCLUSIONS – HOTSPOTS

Use a VPN.

Ensure all station and password security settings discussed earlier in this document are implemented.

Assume someone is monitoring or attempting to hijack your station.

Verify the SSID of a hotspot Wi-Fi with the hotspot administrator, especially when several hotspot WiFi's display on the station's "Networks Available" list.

If not using a VPN, NEVER transmit sensitive data such as passwords, Social Security Numbers, etc.

Make your email password is unique only to your email account. People often use their email password as passwords to other sensitive accounts. Hackers know this fact.

It Is best to change your email password when you arrive home after accessing your email at a Wi-Fi hotspot.

CONCLUSIONS – HOME NETWORKS

Ensure all station and Wi-Fi security settings discussed earlier in this document are implemented.

Install AirSnare, a free application that will look for unexpected MAC addresses on your Wi-Fi network, monitor DHCP requests and notify you accordingly.

Periodically open your router's administration page and access the DHCP Client table (Discussed in Part 2 of this document). Check for unauthorized wireless devices connected to your network.

FINAL COMMENT

I hope this document has helped Roundtable readers to safely use Wi-Fi systems. I've done a lot of research on this subject but am by no means an expert. If any reader has more to add to this subject I would be very happy to receive a response.

This article was written by Bill Rinker W6OAV who wrote and originally published this article in the Denver Radio Club Newsletter and reprinted in the Livermore Amateur Radio Klub (LARK) newsletter in June 2012.

Thank you Bill W6OAV.

73 Ian W6TCP

California QSO Party

CQP 2012
Where were you?

Send your CQP write ups to the JUG editors and have the article published in JUG?

November JUG deadline—28th October!

What to do when you have Power line RFI
Stu Phillips - K6TU

There are two kinds of hams… those who suffer from power line interference, and those who will. Urban, suburban, rural – if there is electricity where you are, at some point you will get RFI.

NCCC territory mostly gets its power from Pacific Gas & Electric (PG&E). PG&E is responsible for maintaining the utility services they provide in terms of quality of service, public safety and compliance with Local, State and Federal regulations.

The FCC has made it clear (over many years) that RFI from power transmission lines that affects licensed radio services (and that include us) must be rectified by the utility company in a "timely manner".

The Commission doesn't define what "timely" means and utility companies have large territories to maintain, budgets and profit levels within which they have to operate and lots of customers to keep happy.

Set your expectations

Many of us have had the experience that "timely" is measured in years or perhaps eons. Complaints get made, some appeasement is attempted but problems often go years without being fixed.

This note describes what you can about this and how to go about getting the problem fixed. Bear in mind that service restoration and human safety issues are the top priorities for PG&E and that the winter season often pushes preventative maintenance down to the bottom of the stack. So set your expectations that "timely" is in months – but after 4-6 months the problem should have been addressed or the issue escalated.

Systemic issues

From personal experience and that of fellow sufferers, it clear that many of the delays in getting RFI issues fixed are systemic in nature. PG&E like many large companies that have been around for a few decades, has many internal systems used to track their business. Apparently many of these systems aren't fully connected to one another and so one source of data may say X, and something else says NOT X. When X = Fixed you can see the problem!

PG&E maintenance is organized in districts or depots. A couple of the larger ones here in the Bay Area are San Carlos and Cupertino. Responsiveness to RFI problems is different between districts with some being more attentive than others.

How to deal with YOUR RFI problem

In theory, PG&E is responsible for locating the source of interference once its reported. As you will see below, when you file an RFI complaint, PG&E will contact you within 10 business days to arrange for a technician to come to your location and scope out the problem.

The first two parts of your problem start here:

- RFI is often intermittent based on weather, time of day, year etc.
- The technician, although often well equipped with test gear to help find the problem may not be the most proficient at using it.

So when you get an RFI problem, it behooves you to make a reasonable effort to isolate the source(s – 'cos there is often more than one). In many cases, your radio theory and training is beyond that of the technician who is dispatched to the field.

For more information on finding the source check out the excellent presentation by Ira K2RD on the NCCC web site at:

http://nccc.cc/members/pdf/k2rd_noise_apr06.pdf

Before you make a report to PG&E, do your best to find the sources. In particular, kill the power to your own location and make sure the noise isn't in your own home! Second, if you isolate the noise down to one of your neighbor's homes, PG&E has no jurisdiction and you need to report the issue to the FCC. Here it helps if you are on good terms with your neighbors but keep in mind liabilities issues if you are on good terms and pin point the problem. It is better for you to recommend a way to fix the problem than fix it yourself. And then there is still the FCC…

The PG&E process

Follow these steps:

1. Do your best to isolate/identify the sources of the RFI. Keep a log of time, frequency, weather conditions, direction if you have a beam AND follow K2RD's advice on finding the problem. It may be straight forward, it's often difficult (keep that in your mind when thinking about the field technician).
2. Call the PG&E 800 number (800-743-5000) and use your own version of the following script: *"Hello, I am calling to report a Radio Interference issue to my FCC licensed radio station."* You may get transferred to another customer service representative who will ask you for details of the problem.
3. Give all the pertinent details and ask that a TROUBLE TICKET is opened. MAKE SURE YOUR GET THE NUMBER OF THE TROUBLE TICKET before you get off the line.
4. Start a time line log of every contact you make including opening the trouble ticket. At every step of the way, write down the date/time, the name of the person involved, the trouble ticket number and a brief description of what happened.
5. Usually #3 above will end up with the CSR telling you that someone will contact you within 10 days to arrange an appointment for a site visit.
6. If no one calls within 10 days, call the 800 number again, give them the trouble ticket number from #3 and ask for a status update. If they tell you there is no such ticket or it has been closed – note that fact

and OPEN ANOTHER ONE – GET THE NUMBER.

7. Once the tech comes out to your location, get his name and ask specifically for what he is going to do next. If he says he is going to open a work order, ask him for the WORK ORDER NUMBER and ask for a date by which you will be notified when work will be scheduled to fix the problem.
8. Now you see why helping finding the problem source(s) is important!
9. Bear in mind that the Trouble Ticket system on the 800 agent's desk appears NOT to be linked to the Work Order system used by the maintenance crews.
10. If a Work order is NOT opened, nothing will be done and you need to repeat step 3 forward again.
11. If the date for repair passes and nothing happens, call the 800 number again and ask for the trouble ticket number status.

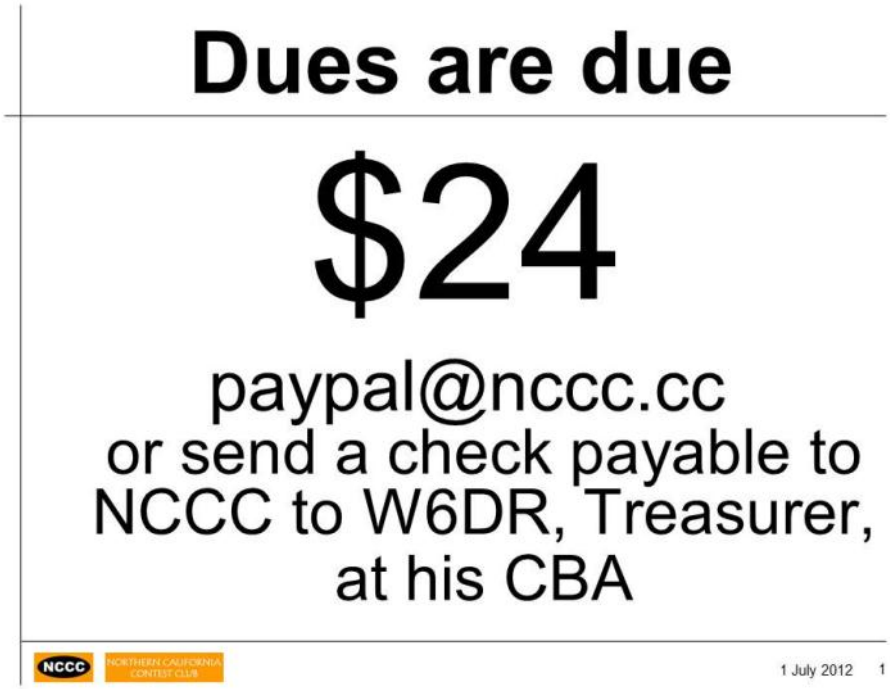
Why all this? Often the trouble ticket gets closed without a work order being entered or completed. I had one case where the crew scheduled to come and fix my problem was diverted to repair an outage and my trouble ticket simply got closed out. I wasn't happy.

Once you go through this process for 3 to 4 months, you have either got the problem fixed (don't laugh, it does happen – think about buying a lottery ticket!) OR you have a wealth of information to escalate the issue.

Next month, I'll describe the escalation process… it too has a number of steps but the final step WILL get action if the earlier ones don't work.

Patience (and perhaps mind-calming exercises like meditation) is your friend! Don't get angry at the CSR on the 800 number – they are just trying to do their job in a sometimes broken system.

Stu Phillips - K6TU



JUG

Please consider writing an article for JUG !

November 2012 Newsletter Deadline—October 28th

This is your newsletter so lets make it something we are proud of. I hope you will consider writing an article for the JUG! Whether its about your station, recent contest experience or a technical article we would appreciate hearing from you.

Send your articles to Ian W6TCP w6tcp@comcast.net and Stu K6TU stu@ridgelift.com