By John Champa,* K8OCL

Communicating Voice, Video, and Data with Amateur Radio

The Hinternet

Protecting HSMM Radio Networks

The 2.4-GHz (13-cm) band presents some unique challenges to HSMM (High Speed Multimedia) radio amateurs. Not only do we share some of the same frequencies (Wireless LAN channels 1 through 6 are within the amateur band), but also we almost always use the same modulation type, IEEE 802.11b/g.

In the years that the former HSMM WG (Working Group) negotiated with the FCC Enforcement Branch via the ARRL's highly experienced attorney, we experimented with many different approaches to avoiding auto-association with Part 15 unlicensed stations. We knew that was one form of communications the FCC did not want to see happen except in the case of an emergency.

What was needed is some effective method of communications isolation or protection called *authentication.* This would immediately identify the Part 15 stations and also immediately restrict them from entering into our Part 97 networks.

First we tried cross polarization. Most Part 15 stations use vertical polarization, so we thought horizontal polarization would provide isolation. That helped somewhat, depending on the situation. However, not all Part 15 stations use vertical polarization, and the multi-path effect causes many polarization shifts that negate the expected isolation.

Then we tried moving out of the WLAN channels range but still within the amateur radio band. Some of our WG called this Channel Zero Experiments. Modification of the repeater (access point (AP)/wireless router) frequency and the modification of the client transceiver (PC card) were both required. However, we were dismayed to find that this wasn't enough of a frequency change. Most standard WiFi PC cards are so broad-banded and unselective that they would auto-associate with Channel 0 gear anyway!

Many other approaches to keeping Part 15 and Part 97 traffic completely separated were investigated. In the end it was concluded that they all added significant overhead to the fledging networks. Either they cost too much, added significant network complexity, or caused a greatly enhance administrative burden, or all of these, thus crippling radio experimentation by Part 97 stations.

The WG finally came to the conclusion that the very methods built into the modulation protocols themselves (WEP, WPA) held the solution. Yes, these are primarily encryption methods, but they also very efficiently and cost effectively provide a poor-man's authentication method. However, the intent is not to obscure the meaning of the transmissions, only to protect the network. With your callsign always in the clear (service set identifier, or SSID), the encryption published and standardized, plus the key recorded in your station logbook, this should be evident to all.

As Les Rayburn, N1LF, Shelby County, Alabama ARES EC recently wrote to me regarding this struggle within:

Like many, I've sat on the sidelines trying to make sense of this hot-button issue: Encryption, especially as it applies to HSMM radio, seems to attract both the best of our technical minds, and the worst of our "barracks lawyers." As an amateur whose primary interest is in emergency communications, I can tell you that security is something that served agencies are concerned about—especially when you're dealing with hospitals and at the federal level, where the Privacy Act seems to creep into almost any discussion.

While we can, and undoubtedly will continue to debate both the technical and legal questions, it's clear that what is really needed is for the FCC to clarify the issue. It might even make sense for us to pursue an exception to the rule that applies to transmissions during emergencies. While I understand the logic of not wanting to see the Amateur Service turned into a common carrier for third-party traffic, it makes little sense for millions of Part 15 users to have no restrictions on encryption, while we as Part 97 users cannot provide even basic levels of security when needed to satisfy our served agencies needs.

As we move into the digital age of amateur radio, our ability to provide backup connections to e-mail and the web will become critical to our role in EMCOMM. We offer a service that is independent of local infrastructure, more survivable than other forms of communication, and more adaptable. All of that may become moot if we can't also offer a service that provides served agencies with the ability to protect information that is transmitted. The other factor is that public service agencies are moving toward P25, and with those moves, we'll likely see more and more agencies opting to encrypt their voice transmissions as well. Once an agency has made the internal decision that OPSEC is important to them, you'll find it very difficult to convince them that amateur radio is an acceptable alternative.

Suggesting alternatives to encryption such as the use of APRS, Winlink 2K, SSB, PSK-31, or other modes provides only the illusion of operational security. Most of these issues are being driven by lawyers, and in a legal sense, these modes are not encrypted or secure. By suggesting that they are, you actually may increase liability for your own group. Certainly these can all provide a level of protection against interception by casual listeners, but I'd be careful of overstating that ability. All it takes is one incident where information that was believed to be secure is intercepted and used for some nefarious purpose. Then all of amateur radio may be tainted by the experience.

For these reasons, and more, we need our leadership to address these concerns with the FCC, and seek rule changes where appropriate to ensure our ability to serve the common good. For those who say we need to avoid the "customer service" mentality, I can understand that position. But the political reality is that public service is the best justification that amateur radio has for its use of the spectrum. You'll never convince a lawmaker that working some rare DX justifies a bigger 60 meter allocation, but you might make the case that we need that piece of spectrum to ensure round-the-clock HF backup links during a disaster.

*Chairman of the ARRL Technology Task Force on High Speed Multimedia (HSMM) Radio Networking; Moon Wolf Spring, 2491 Itsell Road, Howell, MI 48843-6458
e-mail: <k8ocl@arrl.net>

Instead of debating the topic endlessly, I'd encourage amateurs to do something more constructive. Notify your leadership within the ARRL and let them know that this issue is of concern to you. I've communicated my concerns to my section leader, division director, and also to Dennis Dura, K2DCD, who was recently hired as the League's emergency manager. I'm encouraged by his hiring, and also by more amateurs with real EMCOMM experience taking positions of leadership within the League. I think that these important issues may begin to get more of the attention that they deserve. But like any democratic organization, it's imperative that members let their leaders know what issues concern them.

Software Configuration Suggestions

The AP/wireless-router host software is provided with an SSID (service set identifier) which many Part 15 stations turn off supposedly for somewhat higher security. However, radio amateurs should leave it ON. Enter your callsign as the SSID and use it for the station identification. It constantly broadcasts your call in the clear, thus providing automatic and constant station identification.

To be as non-interfering with other services as possible, we need to also look at channel selection. The channels provided under Part 15 are only 5 MHz. However, the 802.11b/g bandwidth is approximately 20 MHz wide. This results in considerable frequency overlap. As a consequence of this, there are only three totally non-overlapping channels: 1, 6, and 11. Channel 11 is outside the amateur Rradio band, so we will focus our discussion only on channels 1 through 6.

Security: It is recommended that you use WEP with a simple key. Remember our purpose here is not to provide encryption, but to enable a simple, cost-effective, and readily available means of authentication. We are not intending to *obscure* the meaning. We are trying to protect the link from Part 15 auto-association or connection—an important distinction! Regardless of what method or level of HSMM radio network protection you decide to use (WEP, WPA, etc.), it should be recorded in your station logbook along with its specific key.

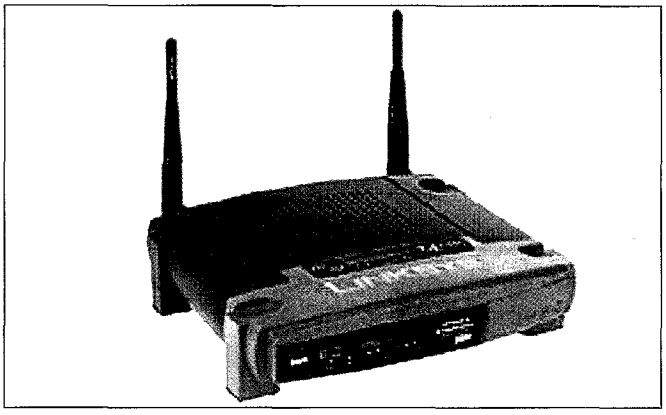
SSID: Again, enabled and with your callsign. It is beaconed periodically for station ID and is always in the clear.

Channel Selection: After you have completed a site survey of 802.11 activity in your area, you will be in a much better position to select an appropriate channel for your HSMM radio link. In the interim, here are some general guidelines: Avoid channel 6. It is the most common manufacturers' default channel setting, and 90 percent or more of your neighbors will be using it for their household wireless LAN. Channel 1 is used by most of the remaining manufacturers as their default channel, so that probably should also be avoided. The result is most radio amateurs use channel 3 or 4, depending on whether there is a WISP (wireless internet service provider) oper-

WRT54GL

Linksys released the WRT54GL in 2005 to support third-party firmware based on Linux, after the original WRT54G line was switched from Linux to VxWorks, starting with version 5.

Version	CPU speed	RAM	Flash memory	S/N Prefix	Notes
1.0	200 MHz	16 MB	4 MB	CL7A	New model line, released after the version 5 WRT54G, which returns to a Linux-based OS as opposed to the VxWorks firmware. The hardware is essentially the same as the WRT54G version 4.0. One alteration is that the internal numbering scheme of the 4-port switch changed in this model, from 1 2 3 4, to 3 2 1 0.
1.1	200 MHz	16 MB	4 MB	CL7B CL7C	In June 20, 2006, this version was shipping with firmware revision 4.30.7. This pre-loaded firmware allows the user to upload a 4 MB firmware image, whereas the pre-loaded firmware on version 1.0 limited the image to 3MB. Firmware version 4.30.11 is now available for both hardware versions. Fully supported by Tomato, openwrt, and DD-WRT.
1.1	200 MHz	32 MB	8 MB	CO61	This is a T-Mobile Special Edition. It is a WRT-54GL (renamed WRT54G-TM). Uses BCM5352EKPBG Chipset and Linux OS. Fully supported by Tomato, openwrt, and DD-WRT. It requires a jtag cable to flash a WRT54GL 1.1 cfe to it, as its stock cfe will reject non T-Mobile/Linksys firmware images. Build the cfe from scratch with your routers' Mac address using "skynet repair kit." After flashing the cfe to it, you can download the Linksys stock firmware for a WRT54GL 1.0 and then use the Linksys web page update tool to flash the third-party firmware onto it. The IP address will go from 192.168.0.1(t-mobile firmware) to 192.168.1.1(WSRT54GW 1.0-1.1 firmware).



ating in their area or not. In that situation, some tactful negotiations may be needed to peacefully co-exist. No, it is not a perfect solution, but at least it is a good faith effort to keep most of your possibly stronger RF signal out of anybody's home or business WLAN.

HSMM Area Surveys

Area or site surveys were mentioned in earlier columns, but we can't put enough emphasis on the need for these surveys *before* you start operating. Exactly how should these be conducted?

Both licensed amateurs (FCC Part 97 Regulations) and unlicensed (FCC Part 15 Regulations) stations use the 2.4-GHz band. To be a good neighbor, find out what others are doing in your area before designing your club's HSMM radio network or long-range Field Day link. This is easy to do using IEEE 802.11 modulation. Unless it has been disabled, an access point/router is constantly sending out an identification beacon known as its SSID. In HSMM practice this is simply the amateur radio station callsign (and perhaps the local radio club name) entered into the software configuration supplied on the CD that comes with the device.

An area or site survey using appropriate monitoring software, for example the free *NetStumbler* software downloaded and running on your PC (http://www.netstumbler.com/index.php), is recommended prior to starting up any HSMM radio operations. Slew your station's directional antenna through a 360-degree arc, and drive your HSMM mobile station (described earlier) around your local area, but not at the same time (hi). This HSMM area survey will identify and automatically log most other 802.11 station activity in your area. There are many different ways to avoid interference with other users of the band when planning your HSMM radio operating. For example, moving your operating frequency two to three channels away from the other stations is often sufficient to avoid head-on QRM.

Basic HSMM Radio Station

How do you set up an HSMM radio base station? It is really very easy. HSMM radio amateurs can go to any electronics outlet or office-supply store and buy commercial off-the-shelf (COTS) Wireless LAN gear, either IEEE 802.11b (now more or less obsolete and usually sold for very low prices) or IEEE 802.11g. There are also amateur radio suppliers of such equipment such as FAB Corporation (http://www.fab-corp.com).

By far the most popular HSMM radio repeater model in use in amateur radio is the Linksys WRT54GL wireless router. It is a combination unit consisting of a wireless access point (AP) or hub coupled with a router. As with other routers, your host PC laptop connects directly to it using a standard Ethernet cable. If the PC is also connected to the internet, then it may also perform the function of an HSMM radio *gateway.* If further, this PC is loaded with appropriate server software, it may also perform a network server function such as e-mail management.

This popular HSMM radio wireless router is a Linux-based model that supports firmware upgrades to distros such as DD-WRT and Tomato (see this URL for details: <http://www.youtube.com/ watch?v=No_NyW2Ug9o>).

If you select the Linksys WRT54GL as your host computer's device, the following link will help talk you through the setup: <http://www.youtube.com/watch?v=No_NyW2Ug9o>.

When you unpackage the AP/router, disconnect both rubber-duck antennas that come with the unit and put them in your parts box or nearest trash container. To connect an outside antenna or even a small field antenna such as the MFJ-1800, you are going to be become familiar with RP (reverse polarity) connectors. These are connectors that may appear to be, for example, male connectors on the outside. However, a close examination of the interior of the connector will reveal that there is no pin. Instead it will be equipped with a socket. Confusing? Not really. How do you get around this situation so you can connect your coaxial cable for the long run out to the tower, etc.? There are two common approaches: (1) use a TNC RP to female N-series adaptor, or (2) construct or purchase a pigtail adaptor with a TNC RP connector on one end and a female N-series connector on the other end.

However, there are *two* antenna ports (used for *receive* space diversity). Which one do you connect to?

The transmitted signal from the wireless router always goes out the same antenna port, except for some Cisco® models that also have *transmit* space diversity. Some access points will allow you to select which antenna port is used for transmission. When one does not allow such choice, you will need to find some means of detecting which antenna is the transmit antenna port with RF output power present. That is the port for the pigtail/feedline connection to your exterior antenna.

Now you are ready to connect your wireless router to the length of low-loss coaxial cable (often LMR-400, equivalent or better) running to the tower, mast, or roof-mounted directive antenna outside. You now have the host end of the link. This is the most complex part of the link. The far end is much simpler. We will cover that in our next column.

73, John, K8OCL