Wireless Digital Nodes

Building a Ham Internet

Atlanta Radio Club Presentation
4/2/2004
Frank Rietta, KI4AWF
Dave Hall, KG4ZGG

Purpose

- Show how an old PC can be turned into an wireless server without being connected to the Internet.
- Show some examples how Hams might be interested in using a server designed specifically for amateur radio that operated on the air.
- The band plans allow hams to modify and operate 802.11b equipment under part 97. More power and range.

Equipment Used in this Demo

- Standard 802.11b wireless cards (Part 15).
- LinkSys 802.11b access point.
- Crossover Cable to connect access point to the server.
- Old computer as the server.
- FreeBSD operating system (Linux will work too).

How to handle proper ID

- The node runs a web server, which can be used as a graphical wireless BBS, a website, or in anyway the Node operator can imagine.

- When a Ham connects, he is required to enter a call sign which is stored in a cookie.

- Notice the footer, it looks like: KG4ZGG DE KI4AWF/D.

Authenticated Radio

- There is a fine line between cryptographic signatures and encrypted data.
- PKI is stands for Public Key Infrastructure.
- Most people use PKI everyday without knowing it; every time you buy something online or use an SSL site, you use PKI!
- PKI can be used with radio without going contrary to FCC rules.

Whats does Part 97 say?

- Section 97.113 (4) "...messages in codes or ciphers ***intended to obscure*** the meaning thereof, except as otherwise provided herein..." (emphasis added).

PGP: Encrypted Message

```
-----BEGIN PGP MESSAGE-----
Version: GnuPG v1.2.3 (FreeBSD)

hQIOA26qQQhVmtQQEAf/ZYuA17TsGubUjNsrbY3kjBvvMpNUcEtMclkAKR7oDhNQ
Ts3xbrIQiOMLZP0GB42gwXqMdNIxVir1wLYszJxbipJLMI/yk5Awg27zrcYXjK3b
2SyTdbaUvReYlsT47ZOKJtxYBHJ3sjg0/vo+MAmDe8yVcU7t5+c0WiCHY5dALkgY
+4ZTIql+kJV4UjdZ9FriVcPhT+CMCez6z6bt+lMBvFxq4I++HojLA9TeAAE/ui5z
zQnIGTPAjKAIsAxFxSGog90/vMHsFcfZT90rXoENNzyEOp+201dZ6N68p1kNBoui
dEATsTQODN7fodIEv6IrWCmRW9PEXFgiVGMTgyxMuwgAjTlgW9rSUNGlbrGWVwsd
/jswPDHSIpSHyxl1gK6hz/LCBpfGzsddUJziyATtK2b/nl3eqPg2b+sQ49p5l236
myCun7dIkgP6imgmuZp2snEy92fJufKK92532zYfMzL5c1mrQJuk3sfVaXXslL3v
iWPtiqlBdBZsmflwiUtUqNza9HASeXCzW529ufpc3FknFNJZ/yYyrQFT5LEeapHq
lLTPF6XDHwXD0AorIPRNGyKXje0upBOAFXBQ8RNxDWRdQBgbGcTo4UqPNc3gUW0X
kP5OK15fAdaZhCQ6UMAekiYuiEebkBX1ooAFoUzCfFwFdFM2fRcDJwW+Wy41HqkO
5tJyAaBWz0emXSaNG6iAbaxu0R+JMxjyIcSE4rTcbZsMY8f8brChcjVJTnwE2gum
oaX51uX3GmexpJi+x9EqmssEsVqVOXe83kvlbtoiXIsXIgAxH15vcqjgi4NDvZmU
540IxIHBpSvIrthYRkIzwGQIUUTn
=ghjG
-----END PGP MESSAGE-----
```

PGP: Signed Message

```
-----BEGIN PGP SIGNED MESSAGE-----
Hash: SHA1

Hello, this is KI4AWF doing a presentation on PKI.

-----BEGIN PGP SIGNATURE-----
Version: GnuPG v1.2.3 (FreeBSD)

iD8DBQFAWvVru9L44h+QFq8RAqNGAJ4pKiBtjMVMPP2Una+Gpvz1Ntp2NACgusOH
Ltg7340+wFoF2yEpHHMNN84=
=uhR/
-----END PGP SIGNATURE-----
```

Encrypted vs. Signed

- A PKI encrypted message both guarantees the source of the message and obscures the meaning of the message (not okay by P.97).
- A PKI signed message guarantees the authenticity of the sender while the meaning remains clear.

IEEE IPSEC Standard

- Standard protocol implemented on all major modern operating systems.
- Allows for both encryption and signing of digital packets.
- ***Packets can be signed, while not encrypted!***

CRAM-MD5 Authentication

- Another form of authentication commonly used in SMTP e-mail servers should also work with ham radio.
- With CRAM-MD5, a server sends a random number which the client uses to encode his password so that the server can verify it but monitoring stations cannot sniff the password.

What could it look like?

Hello KI4AWF, the number is **1234567**.
This is KI4AWF, my authentication token is **8e638a158374d2caba6a5fec5274b3db**.

- The token can only be made with knowledge of the user name, password, and the assigned number, but the meaning is not obscured

- The string was “KI4AWF 1234567 H&m1nT3rnet”.

Band Plan

Moving on in the Spectrum...

802.11b Channel Frequency allocations

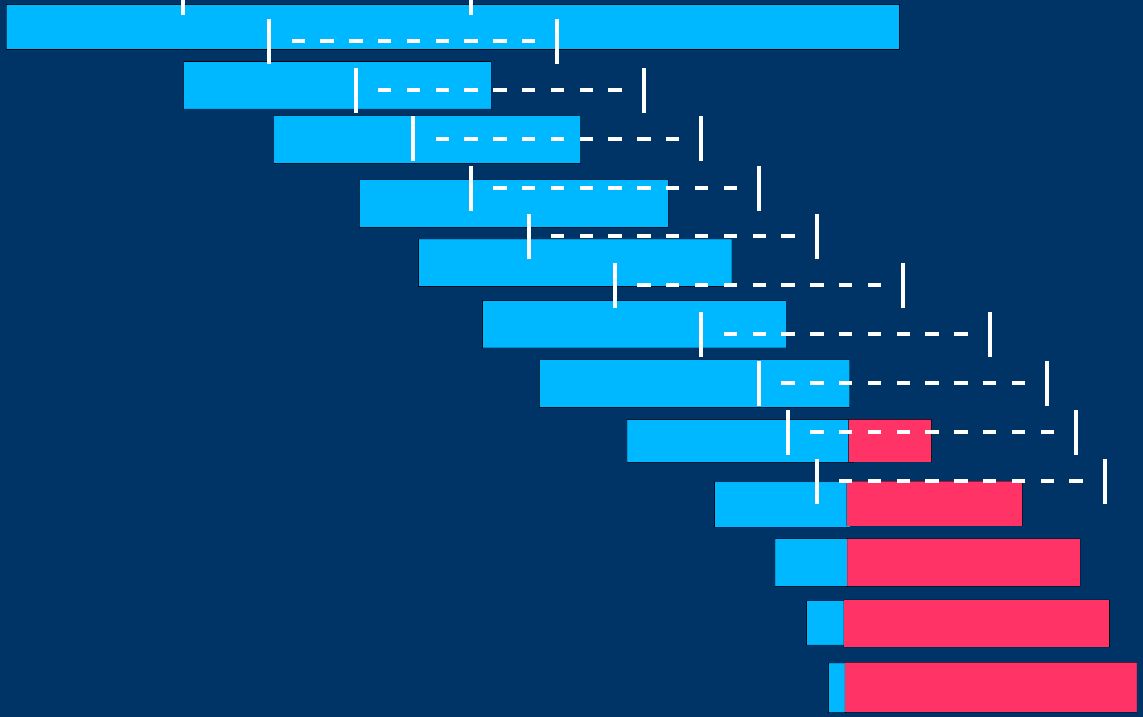
Channel	Lower Frequency	Central Frequency	Upper Frequency
1	2.401	2.412	2.423
2	2.404	2.417	2.428
3	2.411	2.422	2.433
4	2.416	2.427	2.438
5	2.421	2.432	2.443
6	2.426	2.437	2.448
7	2.431	2.442	2.453
8	2.436	2.447	2.458
9	2.441	2.452	2.463
10	2.446	2.457	2.468
11	2.451	2.462	2.473

802.11 and 13cm Ham Band Convergence

2.4 Ghz Ham Band = 2.300-2.310 + 2.390-2.450

```
Frequency   2.39 2.40 2.41 2.42 2.43 2.44 2.45 2.46 2.47 2.48

Ham Band    |--------------------------------|
Channel 1         |----------|
Channel 2             |----------|
Channel 3                |----------|
Channel 4                  |----------|
Channel 5                     |----------|
Channel 6                       |----------|
Channel 7                          |----------|
Channel 8                              |----------|
Channel 9                                |----------|
Channel 10                                |----------|
Channel 11                                 |----------|
```



13CM Band Plan

Obviously the current 13CM ARRL Band Plan was not written with 802.11 in mind, and some level of interoperability with current/future 2.4 Ghz Hams would be necessary

The Current ARRL High Speed Multimedia Working Group suggestion is to encourage hams to limit part 97 802.11 operation to

Channel 6 2.426 - - -2.448

But as this is a large chunk of our 2.4 Ghz spectrum even that will require great understanding a cooperation from/with the current 2.4GHz users within our area.

The Following 4 slides on FCC rules and 802.11 under part 97

Have been stolen from the ARRl Web site with no more then a little reformatting.

Hence Credit should b e given to

Paul L. Rinaldo, W4RI

Manager, Technical Relations

American Radio Relay League

w4ri@arrl.org

John J. Champa, K8OCL

Chairman, High Speed Multimedia Working Group

American Radio Relay League

k8ocl@arrl.net

FCC Part 97 Rules

FCC Part 97.311 Spread Spectrum Rules apply to 802.11b

97.311 SS emission types

- SS emission transmissions by an amateur station are authorized only for communications between points within areas where the amateur service is regulated by the FCC and between an area where the amateur service is regulated by the FCC and an amateur station in another country that permits such communications. SS emission transmissions must not be used for the purpose of obscuring the meaning of any communication.
- A station transmitting SS emissions must not cause harmful interference to stations employing other authorized emissions and
- must accept all interference caused by stations employing other authorized modes.

Thanks to the ARRl Web Site

FCC Part 97 Rules

- When deemed necessary by a District Director to assure compliance with this Part, a station licensee must:
  1) Cease SS emission transmissions;
  2) Restrict SS emission transmissions to the extent instructed; and
  3) Maintain a record, convertible to the original information (voice, test, image, etc.) of all spread spectrum communications transmitted.

FCC Part 97 Rules

- The transmitter power must not exceed 100 W under any circumstances.
- If more than 1 W is used, automatic transmitter control shall limit output power to that which is required for the communication. This shall be determined by the use of the ratio, measured at the receiver, of the received energy per user data bit (Eb) to the sum of the received power spectral densities of noise (N0) and co-channel interference (I0). Average transmitter power over 1 W shall be automatically adjusted to maintain an Eb/(N0+I0) ratio of no more than 23 dB at the intended receiver.

Part 15 Inter Operation

- This is very sticky. Technically, an amateur station using 802.11b could interoperate with an RLAN operating under Part 15 rules. However, communication between FCC Parts is considered a “no-no” Nevertheless, it's possible for an amateur using the same 802.11b card to communicate with an RLAN under Part 15 of the Rules.
- The problem is that a message received over a Part 15 link must be screened for permissible content before it can be introduced into a Part 97 link. However, a proper Part 97 message could be sent on a Part 15 link.
- Confusing? The Rules were not written with any of this in mind.

Antennas

Ham VPN Idea

Closing thoughts

- PKI signatures do not hide the meaning of communication, but enhance it.
- Download PGP for free and start playing with it; www.pgpi.org.
- It will be interesting to create an Atlanta area Ham Network and later connect it with other networks to form a new Ham Internet.