



# PACKET STATUS REGISTER

## In this issue...

President's Corner: FCC & SDRs	1
Kit Supporting T-238	
Weather Station Released	4
APRS Best Practices	5
D-Star Presentation and Demo	6
Basic Password Security	8
TNC-X Is Now Shipping	9
How to Set Up Access Points and Repeater for Home	12

## The President's Corner

# FCC and Software Defined Radios: Danger on the Horizon

By John Ackermann, N8UR, [n8ur@tapr.org](mailto:n8ur@tapr.org)

Those of us who've been thinking for a while about the implications of intelligent radios aren't surprised to see that the FCC has issued a Notice of Proposed Rulemaking (NPRM) on the subject. Its official title is Notice of Proposed Rule Making concerning Cognitive and Software Defined Radios (SDRs) and you can find it on the FCC web site at [hraunfoss.fcc.gov/edocs\\_public/attachmatch/FCC-03-322A1.pdf](http://hraunfoss.fcc.gov/edocs_public/attachmatch/FCC-03-322A1.pdf).



While the NPRM contains some interesting insights, it also contains three paragraphs that pose a grave threat to our exploitation of this new model of radio design. Those paragraphs are important enough that I'll quote them here in full:

*"90. Equipment used by amateur radio operators is generally exempt from a certification requirement. We have maintained this policy to encourage innovation and experimentation in the Amateur Radio Service. However, we are concerned that it may be possible for parties to modify SDRs marketed as amateur equipment to operate in frequencies bands*

*not allocated to the Amateur Radio Service if appropriate security measures are not employed. However, we do not wish to prevent licensed amateurs from building or modifying equipment, including SDRs that operate only in amateur bands in accordance with the rules. Accordingly, we propose that manufactured SDRs that are designed to operate solely in amateur bands are exempt from the mandatory declaration and certification requirements, provided the equipment incorporates features in hardware to prevent operation outside of amateur bands. We seek comment on this proposal.*

*"91. At present there is a clear distinction between radio transmitter technology,*

regulated under Section 2.801(a) of our rules and various radio service rules, and personal computer technology, regulated in a much less restrictive way under Subpart B of Part 15 of our rules. However, increasing computer speeds and speeds of digital-to-analog converters (DAC) may well blur this distinction. A general-purpose computer capable of outputting digital samples at rates in the million sample/seconds range or higher could be connected to a general-purpose high-power, high-speed DAC card that could effectively function as a radio transmitter. The marketing of such computers, DACs, and software to make them interact could undermine our present equipment authorization program at the risk of increasing interference to legitimate spectrum users since none of them would be subject to the normal authorization requirements. At present this is not a problem, but we wish to consider modest steps now to help ensure that this scenario does not become a serious problem.

“92. While such high-speed DACs are presently marketed to the scientific community at high unit costs, we are not aware of any which are marketed as consumer items. We seek comment on whether we need to restrict the mass marketing of high-speed DACs that could be diverted for use as radio transmitters and whether we can do so without adversely affecting other uses of such

computer peripherals or the marketing of computer peripherals that cannot be misused. We seek comment on one possible approach as well as welcoming alternative proposals. Would it make sense to require that digital-to-analog converters marketed as computer peripherals that 1) operate at more than one million digital input samples/second, 2) have output power levels greater than 100 mW and, 3) have an output connector for the analog output be limited in marketing to commercial, industrial and business users as we require for Class A digital devices? Would it be preferable to characterize such systems in terms of output frequency and bandwidth rather than input sampling rate? What sampling rate and power limits would be needed to avoid impacting DACs that might have a legitimate consumer use such as, for video systems and other media applications? Is there a practical way to incorporate security features that would limit the frequency range or other operating parameters of these devices? We also seek comment on the specific types of devices that would be affected and the potential burden on manufacturers.” (Footnotes deleted.)

In short, these paragraphs could result in two serious hurdles for our ability to experiment.

First, commercial SDR hardware could be required to include additional hardware features in order to prevent

transmission outside the Amateur Radio bands. Such requirements are simply incompatible with the idea of a broadband, multi-purpose hardware platform that hams can use as the basis for experimentation. Meeting this requirement would require manufacturers of radios, such as the Flex-Radio SDR-1000, to incorporate additional (and potentially complex) hardware that serves no purpose other than to allow compliance with this proposed rule.

It's certainly understandable for the FCC to be concerned about the interference potential of building-block devices like SDRs that can transmit anywhere within their design range. However, this isn't a new problem created solely by the SDR. Anyone who's looked at a "mod site" on the web will know that many of the radios we buy today can easily be converted to transmit outside the ham bands. SDRs seem to pose little new risk in this area, and the FCC should carefully weigh the harm of increased complexity and cost against the limited benefit of a ham-band-only transmit requirement.

Second, the next two paragraphs of the NPRM address may lead to an even more dangerous problem. Though the FCC again speaks in open-minded terms, it's clear that one possible outcome of

paragraphs 92 and 93 may be to make the high-speed DACs that can create signals directly at RF frequencies unavailable to individuals (e.g., the ham community). These chips are a key part of any vision we have for true software radios that allow unlimited experimentation and novel modulation techniques.

Depending on how the resulting rules are worded, our ability to take advantage of technological advances may be seriously limited. The outcome could range from minor inconvenience to complete unavailability of these parts.

In reading this NPRM and other recent FCC documents (such as the decision on the HDTV “broadcast flag”), it’s easy to reach the conclusion that Amateur Radio has clearly lost whatever special status it once had in the eyes of the Commission. Despite lip service being paid, one could argue that amateurs in the broad sense, i.e., anyone not professionally connected with the communications industry, are no longer seen as a valuable pool of innovators, but rather as a threat.

Is that cynical view warranted? I don’t yet know, but I do know that we have the opportunity to help shape the FCC’s current inquiry through the comment process. Anyone can file comments on an NPRM like this (the deadline is 75 days after the NPRM was published in

the Federal Register, or about March 15). Please read the NPRM in full, and consider making your views known to the Commission. TAPR will be filing our comments soon, but there’s strength in numbers and your voice counts. If we are silent and the rules come down against us, we have no one else to blame.

#### **Tom Holmes, N8ZM: TAPR’s New Treasurer**

I’m happy to announce that Tom Holmes, N8ZM, has taken over the role of treasurer effective January 1. Tom succeeds Jim Neeley, WA5LHS, who served TAPR well in that role for over ten years. Jim has agreed to help Tom with the transition, which will take a few months.

Tom brings significant organizational experience and skill to TAPR. He has held numerous elected positions with the Dayton Amateur Radio Association (the folks who bring you Hamvention) and he has a keen analytical mind. Tom is also an active ham who brings a lot of RF experience (especially at VHF, UHF, and microwaves) to our group.

I can’t say enough about the job that Jim has done for TAPR. The treasurer role is normally pretty low profile (unless something goes wrong!) and requires both attention to detail and sound judgment. TAPR had no financial waves during Jim’s tenure, and that speaks

highly of the job he did. I’m very glad that Jim has agreed not only to assist with the transition, but also to stay involved in TAPR affairs and offer us his wisdom. Thanks, Jim!

#### **It’s Not Too Early to Think about Hamvention!**

Remember that Hamvention is coming up on May 14-16. TAPR will be there in full force, with our usual booth, Digital Forum on Friday morning, and Digital BASH on Friday evening. We hope to see you there!

###

# First Kit Supporting T-238 Weather Station Released

By John Bennett, N4XI, [n4xi@arrl.net](mailto:n4xi@arrl.net)

At the beginning of December, the first kit in a series of two kits offering additional weather sensors and other features to interface with the popular T-238 weather station was introduced. This first kit, the X1W-2 (beta), offers outdoor humidity and temperature sensors. The design is partly based on the now-discontinued 1-Wire Humidity sensor from Dallas Semiconductor. The kit also includes an aspirator (fan) to improve sensor accuracy. Additionally, the PC board is dimensioned and drilled to fit the Davis Instruments Passive Radiation Shield (part #7714). The radiation shield can be purchased from a number outlets for around \$65. The combination makes a very effective sensor addition to a T-238 weather station.

The project entered the design phase in the fall of 2002. My past experience with humidity sensors was not good. They lasted only a few months or the accuracy was very questionable. Cost was also a major consideration. It had to be economical. Commercial grade sensors were in the three-digit price range or higher. After much searching, I decided to use Honeywell's HIH-3610 series. It met all the criteria. The HIH-3610 is the successor to the HIH-3605, which was the type used by Dallas Semiconductor. The HIH-3610 solves most, if not all problems encountered with the HIH-3605.

The first alpha board was placed into operation near the end of December 2002. Since that time, the humidity sensor has proved itself reliable and accurate. Before the kit's release in December 2003, four of the beta units had been in operation for approximately six months with the original in service for nearly eleven months. The original went through a fairly rough winter with no discernible decrease in accuracy or reliability. None in this test group have failed at this point in time.

The second kit to be offered later this year, the X1W-1, will add an array of sensors and other features. The kit will feature barometric pressure, indoor temperature, rain gauge interface, control for an external rain gauge heater, as well as control for the aspirator of the X1W-2. Also, an EMP (lightning) sensor interface will be included with an optional 1-Wire-to-RS-232 converter. The rain gauge interface can be jumpered to accept any type of rain gauge that closes a circuit (e.g., when the bucket tips in the gauge). If desired, the rain gauge interface can be jumpered to function instead as an interface to the Aware Electronics RM series background radiation monitors (support for this will be in my upcoming release of a Linux-based weather server for APRS). Betas of these units are already running at

seven locations here in southern Indiana, western Kentucky, and eastern Illinois and have been very reliable.

You can see pictures of the X1W-1 and X1W-2 betas at [home.insightbb.com/~n4xi](http://home.insightbb.com/~n4xi). Readers might also want to review the presentation that Dwight Hazen, WB9TLH, and myself gave at the Dayton Hamvention. This can be seen at the same web site: [home.insightbb.com/~n4xi/WxnDayton03/index.htm](http://home.insightbb.com/~n4xi/WxnDayton03/index.htm). The presentation includes more information on the development of this hardware and has a large number of pictures of the sensors. I have links on my home page to [findu.com](http://findu.com) for the stations that are using this new hardware. The following sites on the Internet feature real-time data from servers that use many of these sensors: [wshwxn.ampr.us](http://wshwxn.ampr.us) and [wb9tlh.ampr.us/interactive](http://wb9tlh.ampr.us/interactive).

Under consideration is modifying the X1W-2 for a rain-gauge/EMP detector interface. This would allow the option to mount the gauge and/or the EMP detector with the other outdoor sensors. Doing so would eliminate running additional cable for either.

You can purchase betas of the X1W-2 kit from TAPR at [www.tapr.org](http://www.tapr.org).

If you have any questions, I can be reached at [n4xi@arrl.net](mailto:n4xi@arrl.net).

###

# APRS Best Practices for New and Experienced Users

By Chuck Rexroad, AB1CR, abicr@Comcast.net

APRS (Automatic Position Reporting System) is the creation of Bob Bruninga, WB4APR. It is a wonderful mode that has seen explosive growth in recent years. Unfortunately, in many cases, this growth has led to clogged airwaves and an inability to get messages out. Since APRS is a disconnected mode (packets are sent without being connected to another packet station) there is no error correcting.

There are two main types of APRS stations: user stations and infrastructure stations. Infrastructure stations are basically, (a) digipeater nodes that have high elevation and provide wide coverage, and (b) Igates that are typically in the operator's home and receive packets off the air then put them on the Internet. This article emphasizes the proper setup and operation of user stations. User stations can be categorized as either mobile or stationary. The differences in setup are discussed in this article.

There are a number of key parameters that affect the efficient use of the nationwide 144.39 APRS frequency. The two most important are the interval between transmissions, and the path the transmitted signal will take. Since there are so many different software, and even firmware, implementations of APRS, we will not specify

how to set these parameters in this article, but will concentrate on the best practices to select the best possible values to provide good coverage and minimal frequency congestion.

There are two key APRS terms we need to understand before going further:

**Relay** - This is a station with local area coverage that can relay a signal to a wide area APRS digipeater.

**Wide** - This is a wide area digipeater that provides the ability to receive a transmitted APRS signal from great distances.

Stationary APRS stations are by default, setup with an alias of Relay so that they will relay information they hear to the Wide area nodes. Stationary stations should transmit their position no more than twice an hour. Proper setup of a stationary station is to setup the path temporarily as Wide.

If a Wide area digipeater (or more than one) picks up your signal and retransmits it, you should then pick which Wide area digipeater you will use and code that as your path. If no Wide area digipeater picks up your station, try Relay, Wide. Once again, watch to see what stations pickup and relay your signal, then put those call signs in for your path. No stationary stations should use Relay or Wide in their paths; they should use the specific

call signs of the Relay and/or Wide that repeats their packets.

Mobile APRS stations do not have the luxury to setup in the way stationary stations do. Typically a path of Relay, Wide will provide sufficient coverage. If you discover that is not true in your area, try Relay, Wide2-2 that will use a maximum of two wide area digipeaters to retransmit your signal. Mobile stations should transmit no more often than every three minutes if this needs to be hard coded. If a Tiny Trak or other device with "smart beaconing" is used, this time can be computed dynamically based on speed and whether the vehicle is turning or not.

Much of the discussion of APRS is now based on getting information onto the Internet where it can be used by hams and non-hams. The Internet gateways also provide a very convenient way of seeing whether your signal is being picked up and propagated through the system. Web sites like [www.findu.net](http://www.findu.net), [www.aprsworld.net](http://www.aprsworld.net), and others are available and should be used to help fine-tune the parameters for your APRS station to make sure that your getting into the APRS network.

###

# D-Star System Presentation and Demonstration

By Jim McClellan, N5MIJ, jim@mcclellan.net

This past Friday, 12 Dec 03, those of us in North Texas had the privilege of visiting with Matt Yellen of Icom. Matt gave us a presentation and demonstration of the D-Star system, in conjunction with Icom Days at Texas Towers. During the preceding week, we temporarily installed the repeaters, antenna, and a couple of mobile radios. I thought it would help the group to hear about that experience.

In preparation for this event, we had coordinated the digital voice repeater on 1293.0 MHz, with a -20.0 MHz offset, and coordinated the data repeater on 1259.0 MHz. We had also arranged for an Ethernet connection to the radio cabinet. This preparation was done at the N5MIJ 1292.6 site, which is located on a tall building in downtown Dallas.

When Matt arrived in town, he had some pre-production mobiles, and the pre-production repeaters. The mobiles and repeaters looked exactly as they do in pictures posted on the group, and as presented to us at Dayton the past couple of years. We did not yet have the Icom antenna, so we temporarily decommissioned the RP-1220 on 1292.6, and used that antenna. Matt arranged for the Icom antenna and filters to be shipped to us.

On Monday night, Matt Yellen, KB7TSE, Bill Moore, N5ZPR, and Jim McClellan, N5MIJ, installed the data radio, and left the voice repeater powered down. This partial installation provided a great demonstration as to how easy the repeaters are to configure. A computer with USB and Ethernet ports and a few minutes were

all it took.

We set the frequencies of the radios, offset for the voice radio, and an Ethernet address (which is used only in configuring the unit). Things to note: The Ethernet interface on the radio is wired as a hub, and plugs directly into a computer. A crossover cable is required to connect to a hub or switch. The radio has a very short USB cable, and requires an extension. The digital radio acts as a bridge, and is transparent to data operations.

On Wednesday, Bill and Matt again met and installed the system as designed, using the Icom antenna and filters. They also recommissioned the RP-1220 analog repeater. As in all Amateur Radio projects, this took all day. Most of the time was required due to building security and access requirements, not difficulties with the equipment.

Testing on Thursday indicated unacceptable data radio performance. Bill, N5ZPR, again went to the site, and checked configuration and performance. The data radio was found to have an output of only 1 watt, with 10 expected. After several conversations and a few choice syllables, we agreed that the radio would have to be replaced. Matt also confirmed that the Icom-provided filters were tuned to frequencies at a significant distance from our coordinations.

On Friday, Bill, Matt, and Jim returned to the site. It was decided to again decommission the analog system, and use that antenna for the data radio. The voice repeater was left on the Icom antenna, with the

Icom-provided duplexer. We verified functionality with one of the ID-1 mobiles while still at the site. A quick comment about the ID-1 is appropriate here. The radio is completely configurable from either the supplied remote head, or an attached PC. It is much easier to do so with the PC. In the pre-production version of software we used, offsets defaulted to 12 MHz, but were easily reconfigured to the Texas standard 20 MHz. The radio has a lot of memory channels, and each is configurable for standard FM, Digital Voice, or Digital Data. This part was pretty good!

A not-so-quick lunch (another story in and of itself!) and we were back to testing. From Texas Towers, we were not able to directly connect to the data radio at the repeater site. By driving around with a mobile, we verified that the radio was functioning as expected, but that the store was shadowed by several tall buildings in Richardson's telecom corridor a few miles south. We also had to move to slightly higher ground about 1/2 mile away in order to get the ID-1 installed in Jim's Camaro to talk to the voice repeater. This performance correlated exactly with the performance of the analog repeater. Further investigation demonstrated that the performance of the voice repeater could reasonably be expected to correspond to performance of the analog system. The data system does require stronger and cleaner signals, and hence does not get quite the coverage that the voice system does.

Matt gave an excellent presentation of the system's capabilities. Somewhere between 20 and 25 people

turned out on a really cold and rainy evening for this presentation, and asked some really good questions. Matt stood patiently through all of this, and answered all of our questions.

During this week, I saw the following key points:

1. The existing repeater configuration utilizes two radios: a digital voice repeater, and a data transceiver. That's three RF ports with which we have to deal. This is as described, and should not be an impediment. You can use separate antennas, or combinations of duplexers and filters to achieve the required isolation. Do plan appropriately when you work with your local coordinator on this one.

2. The pre-production radios are designed for outside mounting, at the antenna. We're told that the production units should be rack-mounted, which would fit better with most of our installations.

3. The ID-1 mobile radio is a very capable unit. It will talk to the existing analog repeaters, the new digital voice repeaters, and the new data radio. Configuration and operation is easy, once you change paradigms. The ID-1, once programmed, has no need of the control head, mic, or speaker. It turns into the proverbial "black box," with USB and Ethernet ports. One note here: the wiring configuration of the Ethernet on the ID-1 is again as a hub, to plug directly into a PC. A crossover cable is required to connect to a hub or switch. There was one distraction, which we did not identify, i.e., the Call Sign window (which is required to configure the radio) will not display properly on my XP Pro-based Thinkpad. Another notebook, also running XP, did not exhibit this anomaly. We've not yet found the cause of this one...

4. The new digital voice mode offers some interesting possibilities. One really cool feature is that it IDs every transmission, thus eliminating the "Is it time?" question. This ID appears on the remote control head of receiving stations and does not impact the voice transmissions.

5. By "kerchunking" the digital voice repeater with a target of "CQCQCQ" (this is the way most of us will at first operate), the repeater responds with its call sign. This is a great way to answer the "Did I make it?" question.

6. By changing the target to a specific call sign, it's possible to have "personalized & private" conversations.

7. The voice and data operate on separate frequencies. Thus the simultaneous voice and data capabilities do not appear to include the high-speed data. You won't be able to hold conversations on the repeater and surf at the same time.

8. Audio quality on the digital voice repeater is good. While obviously digital and not up to our analog experience, voices were immediately recognizable and easily understood. As expected, signal deterioration in fringe areas makes digital voice unintelligible. Expect to see the same kind of things we all know from digital cell-phones. The codec utilized appears to perform very well, and not use a lot of bandwidth. I was very pleased with the digital voice quality.

9. The existing Icom antenna is sub-par, with respect to our normal expectations of gain and performance. It has only 6 dB of gain, but does have independent antennas for digital voice and data. The Icom-supplied filters were not readily retuned to our coordinated

channels. This required a slight modification to plans, in order to achieve reasonable performance. My expectation is that I'll arrange to get commercially manufactured duplexers and filters, and combine all three ports (digital voice Tx; digital voice Rx; digital data) onto one high-gain antenna and improve both performance and coverage.

10. This one may be the most important thing I saw last week: There's more interest in this stuff than any of us thought. The price points for the equipment appear to be high, when compared to what we're used to spending on mobile radios or repeaters. That same price point is significantly better when you compare the equipment to anything even remotely similar in a commercial product. Even knowing the projected prices, there were still a lot of people that came out on a wet, cold night to see the equipment and listen to Matt. While I've not asked any specifics of the folks at Texas Towers, I do know that at least two of us have committed to purchasing the radios. I'm certain that as we learn more, we'll see more interest, too. As we begin to explore the potential uses for all this new capability, we'll find new ways to do things that we've never even considered.

Summary: The radios are going to be everything we expected. By the time the production units become available, we'll have some truly impressive capability available to us. There will certainly be some bugs through which we have to work. From what I saw last week, both Matt and Icom are committed to getting this right, and to getting it deployed. I think we have some really capable new tools coming!

# Basic Password Security

By Don Rotolo, N2IRZ, n2irz@worldnet.att.net

If you're reading this, you surely have at least one password you need to remember. Most of us have literally dozens of password-protected accounts, and if you're like most humans, you use the same password for almost all of them. That's a problem that you must fix right away.

You might also use a fairly simple password, like "tiger." Or (horrors!) you use a form of your name, birth date, wedding date, user ID, address, or some other easily guessed word. If so, *stop it immediately!* You're setting yourself up for a massive security breach, which will definitely take the better part of a few years to clear up. Imagine if someone, just for one night, had complete access to all your accounts? Ever set a password on a web site to get something (for free!)? You may have just given away the keys to your kingdom.

What you need to do is set up a "strong" password system for yourself. By *strong*, I mean not easily guessed or learned, and by *system* I mean a way of setting a different password for each and every account you have, but without having to remember dozens of different passwords.

Yes, that's right: You need a different password for each and every account. Never ever reuse a password! If that sounds strong, it's meant to. Just like you shouldn't walk alone in New York's Central Park late at night, your basic security is threatened when you use simple passwords, or the same password for more than one account. Read on, it's not nearly as difficult as it sounds...

A strong password is at least 6 characters long (I

recommend 8 to 12 total characters), does not contain all or part of the user's account name (user ID), and contains at least three of the four following categories of characters: Uppercase characters, lowercase characters, digits 0 through 9, and symbols found on the keyboard (such as !, @, #). For example, "strong" is not a strong password, but "sTr0Ng" is.

Come up with a memorable but somewhat random word of about 6 to 8 characters, and make subtle changes to it so that it becomes strong. This will become one of your "core" passwords - you should use different ones for work and home. For example, the word "savings" could be strengthened to "\$a1VngS" - nobody would ever guess that, especially how I misspelled it like that.

Even with such a strong password, using it everywhere defeats the whole purpose. Of course, if you had to remember a different strong password for every single account, you might resort to writing your passwords down - one of the biggest breaches of security you can commit. (If you *do* have them written down, don't. OK, maybe one copy for the safe-deposit box, but that's it! If you pass away, such a list would be useful). Writing them down won't do, so instead develop a system for each account, using the strong core, but making modifications that only you would know.

Here is an example of a password system you could use. I urge you to come up with a variation on this theme, and make that *your* system. In this way, all of your passwords will be strong and it will be very unlikely that someone will be able to gain access to any of your accounts in this way. Even

if they do get one password, the others will still be secure.

Start with a secure core password like \$a1VngS. Take the first two letters of the site name - like "eb" for eBay.com - and add those to the beginning of the strong core. Then, count the number of characters in the site name - four for "eBay" - and add that to the end of the strong core, resulting in "eb\$a1VngS4" for your eBay account, and "pa\$a1VngS6" for your PayPal account. For non-web passwords, you can count the number of letters in the application name, like five for "Excel".

You can see how each account's password will be different and difficult to guess, but easily memorized if you know the system and the core. Please feel free to use the system described, but I strongly recommend making at least some minor changes, such as reversing the letters, or moving the number, or something like that. To summarize, you should *create and use a strong password system wherever possible*.

Oh, one last point related to security and passwords: If you ever leave your computer unattended, such as when you go to lunch at work, either lock your computer (Ctrl-Alt-Del and press Enter for Win XP and 2000) or at least set your screen saver to require a password. That will help minimize the risk of someone getting onto your computer and, say, sending a letter of resignation from your mail account.

Although I hope you enjoyed this short article, it wasn't really written for enjoyment: Security is serious business, and it's really not a lot of effort.



## TNC-X is Now Shipping

*Firmware Is Released As Open Source*

By John Hansen, W2FS, [john@hansen.net](mailto:john@hansen.net)

TNC-X is a new inexpensive 1200-baud TNC kit based on a PIC microcontroller. As a standalone TNC, it is a complete KISS mode TNC on a 2.5 by 3.25 inch PC board that consumes less than 25 mA (about 10 mA if you disconnect the LEDs). It works with any software program that supports KISS mode (*WinAPRS*, *WinTNC*, *PocketAPRS*, etc.).

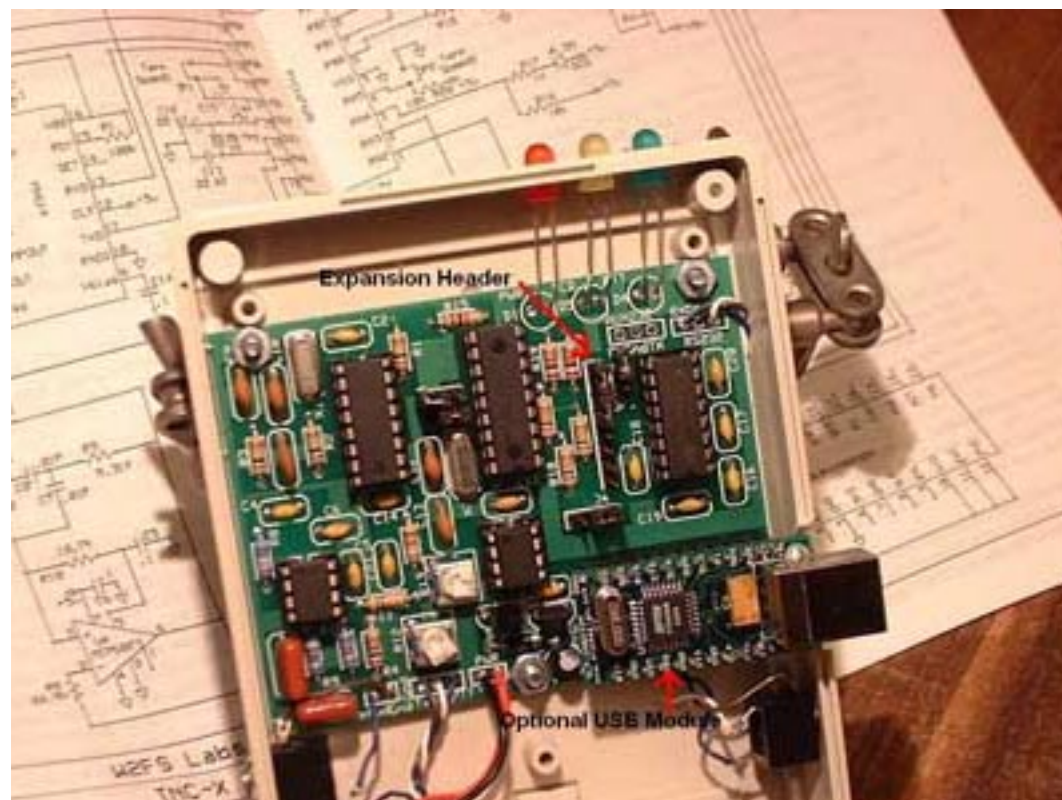
In addition to being a KISS TNC, TNC-X is expandable. You can add a USB port, for example, simply by purchasing a plug-in USB module. Drivers that are shipped with the module make it appear to the host PC as a standard serial port. Thus, PC software that expects to see a serial port on the computer will view TNC-X as being connected to such a port even when the PC has no serial ports, or they are all used by other applications. In addition, when the USB option is used, the TNC can be powered from the USB port of the computer.

TNC-X is also expandable via an expansion header that allows the addition of “daughter boards.” Power is provided to the daughter board through the expansion header. In addition, signals that would otherwise go to or from a host PC can be intercepted by the daughter board at the TTL level and processed. The I/O on the expansion header speaks “KISS” so that any daughter board only has

to send and receive data packaged in KISS to access the core module. This makes the development of daughter boards fairly simple and inexpensive. For example, one could use a PIC (or other microcontroller) to create a daughter board that would convert TNC-X into a standalone digipeater, simply by intercepting the data stream that would normally be sent to the PC, reformatting it (perhaps with call sign substitution), and sending it back out the expansion header. The developer of such a

board wouldn't have to worry about the usual nasty details of CRC calculations, bit stuffing, buffering data until the channel was clear, and timing the bits to be sent to the radio, because that would all be handled by the “core” TNC-X module.

The expansion module also has a second serial port available to it. So it would be a relatively simple matter to develop a daughter board that would take data from a GPS receiver via this serial port, reformat it into MIC-E



frames, and insert this data into the transmit data stream. As yet, no daughter boards have been developed for TNC-X, but that situation should change over the next six months. The expansion header has been used by the University of Hawaii CubeSat project. TNC-X has been selected as the digital interface for this satellite, which has a launch date this coming fall.

### TNC-X is Open Source

TNC-X kits are currently available for \$45 plus shipping from the TNC-X web page: [www.tnc-x.com](http://www.tnc-x.com). However, after a lot of thought and discussion on the TAPR APRS newsgroup, I decided to publish the complete source code. It is written in C and was compiled with the CCS compiler ([www.ccsinfo.com](http://www.ccsinfo.com)). A serious effort was made to make the code as readable as possible, with nearly every line commented. I have also made available the object (.HEX) file and the TNC-X schematic, so you can burn your own chip if you prefer to do that rather than purchase a kit. These files are available on the "documentation" link from the TNC-X web page.

The licensing scheme I selected for this project is the "X-11 license," which is sometimes also known as the "modified BSD" license. It allows the code to be freely adopted by others whether for noncommercial or commercial purposes. This is something of an experiment for me, as I've never tried using open source for any of my other projects. So

far it has been a very pleasant experience. I've already received helpful comments from people who have looked over the source code. Any version upgrades that might result will also be made freely available on the web site.

### Circuit Overview

Complete details of the design of the TNC-X were published in a paper that was presented at last fall's TAPR/ARRL Digital Communications Conference. A copy of that paper is available on the TNC-X documentation web page. There have been a few changes in design since that paper was released and I'm hoping to have a revised version on the TNC-X web site soon.

In brief, incoming audio is processed by an op-amp high pass filter and sent to a CML MX-614 modem chip. In the process of developing the TNC, I discovered that the MX-614 did not perform well in the presence of the low frequency noise that accompanies some packet signals. The high pass filter substantially improves the performance of the modem chip.

TNC-X uses a software DCD and is designed to operate with the radio's squelch open. In addition to ignoring noise, the software DCD also ignores signals on a voice channel and only triggers when actual packets are received.

The TNC requires more memory than is available in the microcontroller itself for two reasons. First, a received packet must be held in memory until the CRC is checked to make sure it has been received properly. If the CRC

checks, it can be forwarded out the serial port. Otherwise it must be discarded. Memory is also needed to buffer transmitted data in the event that the channel is in use at the time that the data arrives at the TNC. TNC-X uses an 8k Ramtron FRAM (FM25640) to supply the needed memory. The advantage of this chip is that data can be transferred to and from it using a synchronous serial protocol. Because this requires only 3 pins for control and data transfer, it permits the use of a much smaller microcontroller than would be needed if parallel data transfer were used.

The microcontroller used in this project is a Microchip PIC16F628A. While it has only 2k of program memory, only three quarters of the memory is actually used by TNC-X. In addition to being physically small, this chip has the advantage of also being very inexpensive. The other chip in the circuit is a MAX232A level conversion chip, which provides true RS-232 level signals to the serial port. Since the MAX232A has two bidirectional serial ports, it seemed like a no-brainer to make the second one available to the expansion header.

The optional USB module is a DLP-USB232M, which is based on the FTDI chipset ([www.ftdichip.com](http://www.ftdichip.com)). While this module is not cheap (\$25), it is very easy to interface to a wide range of projects that would otherwise require serial port communication. The add-on USB kit for TNC-X includes a pre-programmed USB232M and a 24-pin socket. On board

jumpers permit the configuration of the TNC for either the standard serial port or the USB port. This approach has the advantage over using a commercial serial to USB converter, because it permits the TNC to be powered directly from the USB bus. Drivers for the USB module are available from the TNC-X website. Thus far it has successfully been tested with various versions of Windows and Linux. Drivers are also available for the Apple Macintosh, but as yet I don't believe anyone has tested this configuration.

#### Daughter Board Developer Notes

Over the last couple of decades "object-oriented programming" has become all the rage in software development ... and for good reason. Among other advantages, it allows developers with a rather limited knowledge of many areas to develop sophisticated programs. The average Visual Basic developer, for example, doesn't have a clue as to how windows and dialog boxes are actually constructed (at the operating system level), he simply knows how to use them, that is, he understands the user interface. This shouldn't seem strange or magical, though sometimes it does. My wife, for example, doesn't have a clue as to how a modern car actually works (well, ok, I don't either). However, we are both experts at the car's "user interface" so we can use it to get real work done.

This is the basic concept that I had in mind with TNC-X. You don't need to understand

much of anything about the details of the TNC-X firmware to develop daughter boards for TNC-X. All you need to know is this:

1. Five volts is available to you on pin 8 of the expansion header. Ground is on pin 7.
2. You can communicate with the packet engine in TNC-X using standard serial data at TTL level voltages at either 1200, 4800, 9600, or 19200 baud (depending on jumper settings). However, no flow control is supported.
3. The data will come in from TNC-X on pin 3 and can be sent to TNC-X on pin 1 of the expansion header.
4. You have available to you two serial ports. The data on these ports will be converted to RS-232 levels. You can transmit RS-232 data on pins 2 and 5 of the expansion header and receive RS-232 data on pins 4 and 6 of the header. The port on pins 2 and 4 may optionally be routed to the USB port instead.
5. All data that comes in from TNC-X will be in KISS mode. This means the following:
  - a. Each data frame from the TNC will start with C0 00 and end with C0.
  - b. Every time you see the bytes DB DC you should delete them and put in a C0.
  - c. Every time you see the bytes DB DD you should delete them and put in a DB.
6. All the data you send to TNC-X must be put in KISS mode. This means the following:
  - a. Add a C0 00 to the beginning of each

frame and a C0 to the end.

- b. Every time you have a C0 in your data, substitute a DB DC.
- c. Every time you have a DB in your data, substitute a DB DD.

That's about it. You don't have to worry about CRC calculations, bit stuffing, buffering data or any of the other messy details normally associated with constructing packets. Let the TNC-X object take care of all that for you; just focus on the user interface.

So, suppose for example you wanted to build a digipeater daughter board. You have a data stream coming in from TNC-X that will be in AX.25 format wrapped in KISS. You just read it from pin 3 and evaluate the packet header that has the addressing in it. If it meets your criteria to be digipeated, you read it out pin 2, adding your call sign in the from field. While you're at it, you might want to do some work on the digipeater path to improve network efficiency. My point here is that this would be a very trivial project, because the underlying packet engine is already created for you.

If you are interested in developing TNC-X daughter boards, please contact me directly. I'll be happy to provide whatever assistance I can to your project. Note that daughter boards for TNC-X do not have to be created as open source projects, even though TNC-X is an open source project.

###

# How to Set Up Access Points and Repeaters for Home

By Joe Mehaffey, W2JO, [joe@mehaffey.us](mailto:joe@mehaffey.us)

I have wanted to compare the operation of Dlink/LinkSys/SMC bridges and APs to some Cisco products for quite awhile. I recently got a BR342, two AP352s, two BR352s and four AP342s to experiment with. I wish I had tried this gear out sooner! This Cisco wireless gear is great stuff for hotspots, wide area LANs, and use where 802.11b repeaters are needed! Note: These units will only act as repeaters when the central (root) access point is an AP342/352/1100, BR352 or compatible Cisco unit.

I think that anyone thinking about a wide area mesh network (with spans in the range of one mile or less) should consider the use of the AP352E2C (\$300-100mw) and/or AP342s (\$100-30mw) (or later versions such as the AP1100) models instead of the BR342s or BR352s at nodes. Reasons: a) BR342s only work with other BR342s and clients. b) BR342s cost about \$425 and have fewer features than the AP352s at around \$300. And the AP342/AP352 has the same software feature set. c) AP342s and AP352s will interwork and repeat with other AP342s, AP352s, AP1100s, and AP1200s and Cisco says this will continue with the dual channels units coming out.

The potential advantage of BR352s and BR342s is that they can maintain considerably higher throughput on long-range links (greater than a mile or so) than can the AP models. I can confirm that the BR352s will interoperate with other BR352s

plus AP352s, AP342s, AP1100s and clients from a variety of vendors. (Some non-Cisco clients work better than others, but all seem to be able to work at least in non-encrypted mode.) BR352s seem to be essentially AP352s with enhanced software which allows the distance between the BR352 to be up to the range of 60+ miles from remote clients, AP342/AP352s/BR352s with suitable antenna and/or amplifier gain as may be required. The AP versions do have a "range" option but the throughput is down to about 250kbps at 7.5 miles with good signals. Thus, a BR version at the root end of the link will dramatically raise the maximum throughput and range of the link from the root bridge.

The RFLinx 2400CX amps can be used with either model to develop 800mw output (or more with other model amps) if needed for Amateur Radio applications in the 2400mhz ham radio band. One fact called to my attention is that that BR342/352s while operating as repeaters can also provide a data feed out of the Ethernet port. The Ethernet port on the AP342/352s is disabled when they are in repeater mode. Maximum range of the AP units versus the BR units can be an issue. It is reported that max range (from timing considerations) on Cisco's AP models is in excess of 10 miles. (See below for experimental data gathered in this regard.) It has been confirmed that the range of Cisco's AP products is significantly less than the

BR products. Maximum range estimates, based on timing considerations only, for the BR products is said to be in excess of 60 miles. We are checking further and gathering more data to try and discover the precise maximum range limitation on the AP342/AP352//BR342/BR352. Please feel free to email me if you do have definitive information on maximum range for either product!

Now for the downside: The AP342/AP352s have been tested for data throughput when operating in repeater mode over long distances. If the range is less than a mile or so and the signals are strong (SN>25db or so) then you can expect the throughput to drop by half for each repeater the data must traverse. For 11bps this means you have a theoretical maximum data throughput rate something in the order of 5.5 mbps for one repeat and 2.75mbps if traversing two repeaters and 1.375mbps if traversing three repeaters. This is "as expected" as the units are "store and forward" repeaters. However, when I set the units up for operation over a 7.45 mile range, (optimize for range mode), the throughput for two or three repeaters dropped to the range of 250K to 320K bits per second for a wireless file download. See the table below for details. The data rate to the AP when it is used to access the wired Ethernet will be higher as then the central AP is not acting as a repeater, but rather as an access point.

The mesh networking stuff the Cisco gear does

is fantastic! Particularly the new software that has improved self-organizing features. (I am running version 12.04 in six units.)

For ham radio experimenters, the AP352 is a really nice companion to the RFLinx 800mw 17db gain amps located 75 to 100 feet away at the tower top. AP352s start at 100mw (+20dbm) - (75ft LMR400 cable/conn loss=7db) - (pigtail loss=1db) + (amp gain=17db) gives +29dbm which is your 800mw output. Actually RFLinx engineering tells me the 800mw amp will go to +30dbm and that seems reasonable since the amp has a +12vdc PSU and peak voltage at 1-watt output would be only about 10 volts (7vrms). Also, the AP352 has power over the CAT5 Ethernet cable so putting it up the tower with the amp is a little easier than with some other models. (Note: I personally prefer putting the amp at the tower top and the AP gear in a box at ground level. Amps have proved very reliable for me. APs can be temperature sensitive both on the high and low ends of the scale.) The adjustable power output on all these Cisco models is really nice too. And, if you put the amp right with the access point up the tower, you need the 12db amp and 50mw out of your AP to get your 800mw. In the USA, FCC rules for part 15 operation, transmitters are allowed a maximum ERP (Effective Radiated Power) of +36dbm or 4 watts. If you have 800mw transmit power (+29dbm) then you have a net of +7dbi of net antenna gain you can add. "Antenna gain" includes the net of antenna gain and cable/connector loss between the amplifier output and the antenna itself. Note: Generally, it is not in accord with FCC

rules for unlicensed individuals to use amplifiers for 802.11 communications unless the amplifiers are furnished by an equipment manufacturer specifically to work with a given AP/Bridge or such. See FCC rules on part 15 unlicensed operation for details. A word to the wise is sufficient.

Note: The AP342s and AP352s can operate with RF coming out either antenna port in diversity mode unless you select just right or just left. Unfortunately, this is not as flexible as it seems at first glance. While you can get RF out of either the left and right port of these units, the limitation is pretty severe. The access point receives and transmits using one antenna at a time depending on the signal strength readings, so you cannot increase range by installing high-gain antennas on both connectors and pointing one north and one south. When the access point uses the north-pointing antenna, it would ignore client devices to the south.

Interoperability and compatibility tests were run with the Cisco gear and with various brands of client cards. The Cisco units were compatible with 100% of the 802.11b/g cards I tested with. These included Dlink, SMC, LinkSys, Senao, and Orinoco/Proxim. Some problems I noticed follow. (Tests were not all that scientific but I report it as I saw it.)

1) I was using a Dlink 900AP+ as a central AP on my 100ft tower with a 500mw amplifier. Local links were fine, but three links to stations half a mile away through trees had a high error rate in the area of 20%. It had been that way ever since I put

them in and figured this was a result of the dense trees causing multipath distortion. First I put in a AP-342 in place of the Dlink on the tower. One link going a half mile thru trees to a Senao card became completely error free. Things improved on the links with the 900AP+ units, but these links still had errors. Then I noticed that the Dlink 900AP+ units on even some shorter test links had a few errors showing over time. I replaced the 900AP+ with the worst error rate with a LinkSys WET11 and immediately, the error rate went to about zero and has stayed there. I then replaced the other two 900AP+ units with WET11s and those links became error free as well.

2) I have one AP352 acting as a repeater installed about 3/4 mile from my tower with an 8db omni antenna and amplifier. It worked fine from the first moment. I added the 12db amp to get the power up to about 600mw (including cable losses) so as to be able to extend coverage to another repeater and it is all doing a good job.

3) Throughput of three Cisco units in series (AP > repeater1 > repeater2) is still faster than the download speed of a single 1.5mbps ADSL line. (When the distance between units is less than a mile and the units are all set to "optimize for throughput".)

4) Features I like in the Cisco AP342/352 include:

- a) Each unit keeps records of who is connected and logs traffic, errors, etc.
- b) AP342/AP352 has transmit power available on both antenna R-TNC antenna ports. See Note.

c) AP342 converts easily to external amp use by inserting a MMCX plug into the internal PCMCIA card and bringing out the cable to an outside connector. Some AP340 series units have R-TNC connectors on the rear instead of captive antennas, but I have not seen any of these for sale on eBay.

d) You can update firmware by radio (and automatically to all units at once if you want).

e) Everything seems to be adjustable/configurable. (This can be a hazard!) For instance, if you check: "Make unit maximum compatible with standard 802.11 devices", the repeat mode and lots of neat features quit working!

f) It is possible to configure the units so that you can simultaneously serve some clients with encrypted links and others with unencrypted links.

g) These units work with all of the 802.11b/g wireless clients I have tested them with including various SMC, LinkSys, Dlink, Senao, and Orinoco cards and bridge clients.

h) The rated temperature range of some models is 0 C to 50 C. (While the specification is not quite good enough for outdoor and attic use, I find that some units will operate considerably beyond this specification. One unit has performed flawlessly down to 22F and up to 130F. Another quit passing data at about 30F and did not recover when the temperature came back up. On this unit, when failed, you could communicate with it via the Ethernet connection, but I had to unplug/replug the Ethernet cable to bring it back to operation.)

i) You can program all features remotely (and

securely) by radio. This includes cases where you have multiple signal repeaters.

j) If you have two or more "source" feeds from the Internet, the units will self organize. Load balancing is apparently manual but any section of the "mesh" where the primary feed fails can "home" on another mesh section where AP service is still working.

k) The "associated" table shows "who is connected to whom" including clients, repeaters and access points. (I have noticed that client NICs rather than client bridges are what show up in the associated table where you have (say) a WET11 client bridge connected to a NIC card in a client computer.)

l) You can set up the Cisco units to prevent peer-to-peer connections on the local wireless LAN if you want. Couple this to "per client" bandwidth throttling (and Kazaa, etc throttling or blocking in a Mikrotik hotspot) and you can control your gamers and music sharers and keep them from overloading your network. As you can tell, I really am impressed with the features of the Cisco gear and the AP342 is really cost effective at \$100 or so on eBay.

### How to Setup the APs for Optional Encryption and as Repeaters

First: A few "gotchas" to keep you from being confused.

1) Your AP <must> be in AP mode for you to communicate with it over the Ethernet cable. This is the default, but once you put the unit into "repeater access point" mode you have to communicate with it via the radio channel. So: Do not put the unit into repeater AP mode until you have made sure

you can communicate with it by radio as an AP.

2) If you plug the unit into your computer's LAN port, and the unit is then configured as a root access point and programmed to revert to "repeater access point" mode when it loses contact with its router over the wirelan, it will disable communications with your computer over the wirelan cable as soon as you enable the "revert to repeater access point when communications is lost" mode.

3) Pushing the AP342s reset button for 10 seconds loads the default parameters. The AP352 has a hole for a reset button, but the reset button is missing. There is no way to reset an AP352 to factory defaults without using <:RESETALL> from the *HyperTerminal* command line interface if you lose connectivity for some reason. I did this a lot early in my experimentation.

4) Use *HyperTerminal* and 9600,8,none, 1, hardware with a 9 pin serial cable to connect to the APs to discover their IP address initially. Just turn the unit on with *HyperTerminal* connected and you will see the IP address (and lots of other stuff) during boot up. After you have the unit's IP address, connect a LAN crossover cable between the computer and the AP. Then set your computer's IP address to some other IP address in the same range but different from the AP. Then load a browser and you should be able to <http://<AP unit IP address>> and you should be able to connect to the AP setup initial screen.

5) As soon as you get the system up and running and can get to the setup screen, I recommend you go download the latest production firmware for

your units from the Cisco web site (above), unzip it into suitable folders, then go to Cisco services in the Setup Screen and update the firmware. Use the browser update method, as it is most straightforward. Depending on which software comes in your unit, some of the features below may not appear if you do not have the latest software.

6) If you set up your root AP and repeater APs as described below and with encryption "optional", things work almost exactly as you would expect. Individual stations can login and get access if they are unencrypted or if they are encrypted and are using the correct encryption codes. Special note: Sometimes when you set an individual station to be encrypted, that station becomes "invisible" to all other stations on the wireless LAN. This seems to be related to brand/type of client card used. This "stealthy" encrypted station a) can no longer be pinged, b) can no longer be discovered by an IP address scanner, and c) can no longer be accessed by remote control programs such as VNC. And. This is independent of if the remote management station is encrypted or not. This is quite an annoyance. Please see the table with more test data at the end of this article. If anyone knows a setup arrangement for the AP340/350s that will overcome this limitation, please let me know.

7) Pick an RF channel for your APs and repeater APs and do not let them roam the available channels. (See more below).

8) No. It is not possible to use the AP342/352s as repeaters and get a wired LAN signal for local use out of the repeater AP at the same time. In

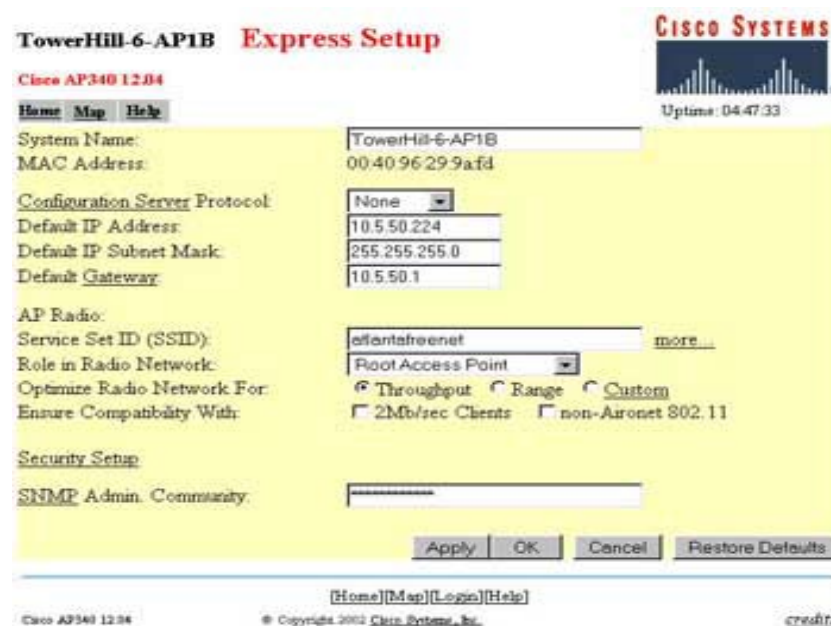
fact, these units cannot be used as a standard wired Ethernet client bridge (receiver) at all excepting for the client feature that is really not what these devices were designed for. BR342/BR352 units do have a wired LAN output available when they are being operated as Repeater APs.

9) The bridges have a range parameter. It appears this has to be set reasonably carefully to match to range to the bridge most distant from the root bridge. At one point, I set the root bridge to 40km range and only had throughput to another BR352 located nearby (500ft away) of about 3.5kbps. Changing the range setting on the root bridge to zero made the throughput come back up where it should be. The nearby APs that were associated with the root bridge seemed unaffected and appeared to maintain their normal throughput speed independent of the range parameter. (But we know making the range parameter a large number does cut down on the total throughput of the bridge. My future testing should define some values for this reduction.) It appears that running nearby APs and distant BRs from the same root BR could drop the overall throughput capability of the root BR significantly. Can someone with experience comment on this please?

Now to the setup itself

How to set up the Cisco AP 342/352s was somewhat mysterious at first. There is a pretty inclusive AP342/352 FAQ web page and relatively good manual that is downloadable from the Cisco web site. Note the help link near the upper left of the page (below). This brings up a help file link from the Cisco web site (assuming your AP has internet access). All this documentation got me started pretty well. The screen photos below were made with an AP342, but the AP352 setup is almost identical except for the RF power settings. I was able to get the unit working as an access point by only going to the express setup page and inputting my IP address, SSID and other information as follows.

Figure 1 (below) shows the express setup screen for an access point.



**TowerHill-6-AP1B Express Setup**

Cisco AP340 12.04

Home Map Help

System Name: TowerHill-6-AP1B  
 MAC Address: 00:40:96:29:9a:fd

Configuration Server Protocol: None  
 Default IP Address: 10.5.50.224  
 Default IP Subnet Mask: 255.255.255.0  
 Default Gateway: 10.5.50.1

AP Radio:  
 Service Set ID (SSID): effortstheenet more...  
 Role in Radio Network: Root Access Point  
 Optimize Radio Network For:  Throughput  Range  Custom  
 Ensure Compatibility With:  2Mb/sec Clients  non-Aironet 802.11

Security Setup:  
 SNMP Admin. Community:

Apply OK Cancel Restore Defaults

Home Map Login Help

Cisco AP340 12.04 © Copyright 2002 Cisco Systems, Inc. credits

There are a couple of things to note about the above:

1) The system name is arbitrary and should be something meaningful to the system operator.

2) The configuration server protocol options are NONE, BOOTP, and DHCP. You use NONE if you want to use a fixed IP address. You use DHCP if you want the LAN router to pick an IP address for you. BOOTP I do not know much about. It makes it a lot easier to administer the AP if you have a fixed IP address that you can easily refer to.

3) The SSID can be whatever you want for your particular installation.

4) "Role in Radio Network" is a little tricky if you intend to use some units as repeater access points. Root access point means the unit is going to have a wirelan connection and will operate (more or less) as a conventional AP. Repeater access point means the unit is going to not have a wirelan connection and will operate as a repeater for other Cisco APs configured as root access points. Site survey client means you can configure the AP for site survey use as a client but it is pretty clumsy at that task. The tricky part is that even if you want to use a particular AP as a repeater access point, you really want to configure it here as a root access point. The reason is: a) it allows you to program the same AP functionality into all your APs and b) coming soon (below) is an option that you can set that will direct the root access point to become a repeater access point whenever the wirelan is not present. By this arrangement, any Root AP is interchangeable with any repeater AP without any adjustments. Also

note: You must (in version 12.04) be connected to a wire Ethernet link or you will not be allowed to change the role from repeater access point back to root access point.

5) For the "Optimize Radio Network For" question, I recommend as follows: maximum desired range less than 1 mile, use throughput. Range more than one mile, use range. See information on range tests done (near end of paper) for more details.

6) Leave the "Ensure Compatibility With" options unchecked. If you check these, many of the neat AP342/352 features (such as repeating and optional encryption) will disappear. (I found this out the hard way.)

7) If you are using SNMP management features, insert your administration community ID here.

Bridges (as opposed to access points) are a little bit different in that BR342 and BR352 have a few more options.

Another setup screen you need to consider is the Ethernet Hardware Setup Screen (below).

Assuming you have multiple APs and/or some repeater APs, set the "Loss of Backbone Connectivity Action" to <Switch to Repeater Mode>

This will cause the AP to operate as a standard access point unless/until the AP loses the wirelan connection and then it will switch to repeater AP

**TowerHill-6-AP1B Ethernet Hardware**

Cisco AP340 12.04

Map Help

Speed: Auto

CAM Size: 0

Loss of Backbone Connectivity # of Secs (1-10000): 2

Loss of Backbone Connectivity Action: Switch to repeater mode

Loss of Backbone Connectivity SSID: atlantafreenet

Apply OK Cancel Restore Defaults

Cisco AP340 12.04 © Copyright 2002 Cisco Systems, Inc. credits



mode automatically and associate with a nearby AP and continue serving local clients. If your main AP(s) cannot operate as a repeater for a nearby client, you likely will want to select “shut off the radio” option in case the wireless link fails. Otherwise, the strong radio signal from the failed AP may continue to link to local clients instead of dropping the RF link and allowing local clients to roam to another AP.

### Notes

1) For the best results where you have multiple root access points, do not leave the loss of backbone connectivity option set to “No Action” on your root access points. If you do so, in case of root AP failure, repeaters associated with this root AP will not roam to mesh with the remaining “still alive” APs and repeater APs on your network. You may select from change to repeater mode, shut off radio, or restrict to SSID. No action will work fine if you have but one root access point or bridge.

2) Bridges have the same loss of backbone connectivity options as APs. However, with bridges, I suggest you do not set the loss of backbone connectivity option to change to repeater mode. If you do set to this option, then your bridge may find another root bridge or root access point to associate with if it loses connectivity on the wired LAN connection. If it does associate with another node and become a repeater node, the Ethernet port becomes an output from the bridge instead of an input to the bridge and you cannot regain control when you recover your Ethernet connectivity to the bridge without cycling power on the bridge unit.

This can lead to some very confusing symptoms when data from some remote network starts appearing on your local hub or switch through the bridge’s Ethernet port.

Below is the “Radio Hardware” setup screen. There are a few adjustments you may want to make. But you may be happy with the default settings as well.

You will have already set the SSID when you arrive at this page if you do the express setup. You do want the broadcast SSID to associate and likely you do not want to allow “just any old SSID” to associate which will occur if you set “world mode” to yes. Note the “more...” link to the right of the SSID window above. If you want, you can set up multiple SSIDs for each unit. This can be

## TowerHill-6-AP1B AP Radio Hardware

Cisco AP340 12.04

[Map](#) [Help](#)

Service Set ID (SSID): atlantafreenet [more...](#)

Allow "Broadcast" SSID to Associate?:  yes  no

Enable "World Mode" multi-domain operation?:

Data Rates (Mb/sec):

1.0  2.0  5.5  11.0

Transmit Power:

Frag. Threshold (256-2338): <input type="text" value="2338"/>	RTS Threshold (0-2339): <input type="text" value="2339"/>
Max. RTS Retries (1-255): <input type="text" value="32"/>	Max. Data Retries (1-255): <input type="text" value="32"/>
Beacon Period (19-5000 Kusec): <input type="text" value="255"/>	Data Beacon Rate (DTIM): <input type="text" value="2"/>

Default Radio Channel:  In Use: 5



Search for less-congested Radio Channel?:  [Restrict Searched Channels](#)

Receive Antenna:

Transmit Antenna:

If VLANs are *not* enabled, set Radio Data Encryption through the link below. If VLANs are enabled, Radio Data Encryption is set independently for each enabled VLAN through [VLAN Setup](#).

[Radio Data Encryption \(WEP\)](#)

Uptime: 04:54:16

used where you want your own SSID transmitted (primary) but want the unit to respond to one or more alternative SSIDs as well. Note that the SSIDs are case sensitive. In my own area, I set up my primary SSID as <atlantafreenet.org-W2JO> for station ID and added <atlantafreenet.org> and <ATLANTAFREENET.ORG> as a second and third SSID for compatibility with the AtlantaFreeNet.Org conventions. This way I can tell my own hotspot system from the other AtlantaFreeNet.Org systems but my hotspot system will still respond to the “standard” AFN SSIDs.

The transmit power is adjustable (max 30mw AP342/100mw AP352). This adjustment can be used to adjust power downward if you have an external amplifier and would be overdriving it with the max power setting. Be careful about the calculations of drive power required when using amplifiers. If you put too much drive into an amplifier, not only will the overdrive create distortion on your signal and actually reduce your range capability, it can cause severe interference with other users of 802.11 equipment and get you a visit from the FCC!

The default radio channel setting is 6 and with search for a less-congested radio channel =yes. I suggest you pick a fixed channel setting for all your APs, turn off search for less-congested channel and stick to it. I tried allowing the system to “roam” and some of the repeaters would “get lost” and stay on the “default” channel where the access points were not available. I saw no significant throughput degradation from having two root APs on the same

channel.

The receive and transmit antenna settings can be set individually for left, right or diversity. If you are using the unit as a normal AP with its built in antennas, you will likely want to use diversity for both. If you are connecting the unit to an external antenna or amplifier, you will want to select left or right depending on which port on the unit you choose to connect to your antenna. Remember that the access point receives and transmits using one antenna at a time, so you cannot increase range by installing high-gain antennas on both connectors and pointing one north and one south. When the access point used the north-pointing antenna, it would ignore client devices to the south.

### Wireless Encryption Setup

There is a really neat feature in the encryption capabilities of the AP342/AP352 units. Access points can be configured to serve both encrypted and non-encrypted clients simultaneously. This is done with the “Encryption Optional” setting on the WEP setup page (below).

### Notes

1) You must put in the WEP key size and then the WEP key before the “Use of

Data Encryption by Stations” options will appear.

2) The data encryption options are: a) no encryption, b) optional, and c) full encryption. Optional means that a station logging on with no encryption will be allowed and if a station logs on with the correct key he too will be allowed to associate and the second station’s send/receive data will be encrypted using the selected WEP key.

3) Keys must be input as hex digits. Key 1 is the transmit key and must be entered. The others are optional.

4) The encryption functions above apply when the AP342/352s are operating in any mode. When

**TowerHill-6-AP1B AP Radio Data Encryption**

Cisco AP340 12.04

Uptime: 05:48:17

IF VLANs are *not* enabled, set Radio Data Encryption on this page. IF VLANs are enabled, Radio Data Encryption is set independently for each enabled VLAN through [VLAN Setup](#).

Use of Data Encryption by Stations is: **Optional**

Accept Authentication Type: **Open**  **Shared**  **Network-EAP**

Require EAP:

Transmit With Key	Encryption Key	Key Size
WEP Key 1: <b>C</b>	<input type="text"/>	128 bit
WEP Key 2: -	<input type="text"/>	not set
WEP Key 3: -	<input type="text"/>	not set
WEP Key 4: -	<input type="text"/>	not set

Enter 40-bit WEP keys as 10 hexadecimal digits (0-9, a-f, or A-F).  
Enter 128-bit WEP keys as 26 hexadecimal digits (0-9, a-f, or A-F).  
This radio supports Encryption for all Data Rates.

Apply OK Cancel Restore Defaults

the units are in repeater access mode, some special considerations apply. If the repeater AP is set for no encryption, then all the traffic it passes will be limited to unencrypted traffic. If it is set to full encrypted the repeater will only be able to pass encrypted traffic so the associated root AP must be set to either optional or full encryption for this repeater to operate. This tidbit confused me for awhile as I had been told that if the root AP and repeater AP were set to encrypted, then all "inter-AP traffic (even unencrypted) was encrypted between the AP and repeater. This appears not to be true.

I am still figuring out the details about how all this mesh networking gear works. Helpful hints, corrections, suggestions and pure criticism all accepted in the spirit of "getting it right"!

Thanks

Joe Mehaffey

See also our article on how to setup a MikroTik HotSpot Router ([www.gpsinformation.org/hotspot/mikrotik\\_hotspot\\_article.html](http://www.gpsinformation.org/hotspot/mikrotik_hotspot_article.html)).

See Also the AtlantaFreeNet.Org Web site ([www.atlantafreenet.org/home.php](http://www.atlantafreenet.org/home.php)).

And also our "home base" GPS Information Web site ([gpsinformation.net/](http://gpsinformation.net/))

Tight VNC Remote Control Compatibility Tests With Various Client And Server Radio Cards/Units

VNC client is in all cases connecting through one or more AP342s in these tests to a remote VNC server. VNC client can connect to these client units/cards in systems running VNC server as

shown below (yes or no).

VNC Client	VNC Server	VNC Server	VNC Server
Senao (encrypted)	Senao(not enc) =yes	Linksys Wet11 (not enc)=no	WET11(enc)=yes
Senao (NotEnc)	Senao(Not enc)=yes	Linksys Wet11(not enc)=yes	WET11(enc)=no
LucentGold(NotEnc)	Senao(Not enc)=yes	LinksysWet11 (enc)=no	WET11(NotEnc)=yes
WET11 (NotEnc)	Senao(Not enc)=yes	LinksysWet11(NotEnc)=yes	Wet11(enc)=no
WET11(enc)	Senao(Not enc)=yes	LinksysWet11(NotEnc)=yes	Wet11(enc)=yes

If the receiving (VNC Server) Senao card is set to encrypted in the tests above, the receiving Senao card "disappears" from view on the wireless LAN. It cannot be pinged, found by an IP scanner or by the VNC client machine from any wireless station. In this situation, the Senao card does have normal connectivity to the Internet, to mail servers, and etc. This "stealthy" behavior was a surprise.

Anybody care to explain the table above? I cannot explain why some devices (Senao) as receivers for the VNC servers will operate with the sender encoded or not, whereas other combinations do not. In any case, it seems that the key is that consistent results are achieved when both ends of the VNC connection have encryption on or off. Except for the Senao card that loses connectivity with all but the wired LAN when it is set to encrypted and run through the Cisco AP342/352. My guess is that this is the result of the specialized Cisco protocols used for relaying and other purposes not being 100% compatible with standard 802.11b gear.

What you see in the MAC/IP address displays of Cisco AP342/352/BR352s is not always exactly

what you expect.

The association display tables of the Cisco APs do not always display all of the connected IPs and MAC addresses alive on the network. The main discrepancy appears to be when an external wireless client bridge (such as the LinkSys WET11 or the Dlink 900AP+) is used to provide a radio-to-radio bridge for a client computer. In such an arrangement, there are possibly three sets of MAC addresses and IP addresses to consider. These are: a) The MAC address and IP address of the LAN card (NIC) in the client computer, b) the IP address and IP address of the Ethernet side of the client bride device and c) the IP and MAC addresses of the wireless side of the client bridge device. With this array of addresses to choose from, here is a table showing what is actually displayed by various devices/software on the hotspot network. Note: In this example, all client bridges (WET11s) and Cisco APs have fixed IP addresses and all client NICs use DHCP. DHCP scanning by the Mikrotik Hotspot's DHCP server does not cover the range used by the fixed IP address devices and this may be the cause of

the fixed IP addresses not showing up in the Cisco AP tables. Though why they sometimes show up in the Cisco association table is still mysterious.

(Firmware in use is Cisco version 12.04) maximum range confirmed greater than 7.45 miles

	IP displayed	MAC displayed	IP/MAC when Mikrotik Auto MAC Login enabled
Device			
Client WinIPCfg	NIC	NIC	
Bridge Utility SW	WET11	WET11	
Cisco Association	NIC (sometimes WET11 also)	NIC(sometimes WET11 also)	
Mikrotik HotSpot Active	NIC (but not if WET11 in circuit)	NIC(but not if WET11 in circuit.)	IP/MAC of autologin via MAC NIC clients now shown in MT version 2.7.19
Mikrotik Router DHCP server leased	NIC	NIC	NIC
Mikrotik			

### Notes

1) This table data is still being developed. More details to follow.

2) The older WET11 hardware with firmware version 1.54 appears to be fully compatible with Cisco APs tested here. However, the newer WET11 hardware with firmware version 2.07 will not link to Cisco AP342/AP352 units with multiple SSIDs enabled. Version 2.07 firmware was supposed to fix this but it did not. Other than this, the WET11 continues to be a quality, inexpensive, and easy to use wireless client/bridge unit.

Experiments to Determine the Maximum Range Capability of the AP342/AP352

Experimental data gathered thus far as to the maximum range of the AP342/AP352 is given below. These experiments were run with a two-watt amplifier on each end of the circuit with a combined antenna gain of 17db for the duration of the tests. This was done so as to insure to the extent possible that RF signal level is not the determining factor if data rate slowdowns occur on the link. There are two configurations to consider. These are AP optimization set for throughput (TP) and AP optimization set for range (RG). Note: The author is an Amateur Radio operator and is licensed by the FCC under FCC part 97 to operate at higher power than that allowed for part 15 equipment for experimentation on the section of the Part 15

frequency range that overlaps with and is shared with the Amateur Radio service. Unless you hold an Amateur Radio license you would be operating illegally and outside the Part 15 and FCC rules to use power levels not provided by your FCC Part 15 approved equipment.

Now to the measurements

1) Out to at least 1.5 miles, the APs will work in TP mode but the speed is down to 2mbps at 1.5 miles with good signals. Changing the setting to RG mode gets the speed back up to 11mbps at 1.5 miles. I am sure that there is actually a compromise of the overall data transfer speed, but it is nice to see the bit rate return to 11mbps when the RG option is selected. I am not sure where the optimum crossover occurs, but if you are over about 0.75 mile between a base station and repeater or between repeaters, you should try the TP and RG options and see which one works best for you based on sustained data throughput

2) Out at 3.7 miles from the base station (with considerable trees in the way on the mountaintop), signals were at 42% on the AP342's signal strength display. On RG option, the bit rate was 11mbps and the system operated very well indeed. I changed the settings to the TP option and the speed went to 1mbps and I was (just) barely able to pass enough data to the base station's AP342 to change the option back to range. So. I think that something in the range of a mile or a bit less is the place where you should change the AP's option from TP to RG.

3) Out at 7.45 miles from the base station (in the car on local Sawnee Mountain, this time

with drizzle and “moderate” tree blockage in the direction of the base station) signals were at 43% to 53% (varying) with the AP342 operating in repeater AP mode in the back seat of my car. The signaling rate shown in the car and in the AP342 in the base station stayed at 11 Mbps. This was very encouraging. I tried downloading files and everything went along at the max ADSL rate of about 150Kbytes per sec. Performance looks good now out to at least 7.45 miles with the AP342/AP352 equipment. I also tested a Senao client card back to the base station direct (without use of the AP342 repeater in the car) and it performed perfectly as expected as well. These tests were run in the “optimize for range” option both in the base AP and in the repeater AP. No special selection was made in the Senao PCMCIA card setup. Transmit power on both ends was set to 2 watts for this test. Combined antenna gain was about 17db.

4) More distance tests are coming. Keep tuned.

Data Throughput Tests: Direct and Repeater Modes

Of interest to experimenters is the manner in which data throughput is affected by range and the various operating modes of Wireless Data Repeaters such as those of the Cisco AP352/AP342 line. (Note: The performance of other brands and models of wireless equipment will differ and no generalized conclusions should be drawn from this limited data.)

The Setups Used:

<at Sawnee Mountain>-----<at Silver City/Ham Tower>-----

<inside House>-----<inside house>

A) Computer #1+amp~7.45 miles~Cisco AP342+amp~300ft~Cisco AP342 (no amp)~20ft~Computer #2

B) Computer #1~5ft~Cisco AP342+amp~7.45miles~Cisco AP342+amp~300ft~Cisco AP342~20ft~Computer #2

Note that the A setup includes Computer #1 Senao PCMCIA card coupled to a 2 watt amplifier communicating directly to the Cisco AP342 equipped with an amplifier and operating as an Access Point. Then the access point is communicating to a repeater access point located 300 feet away and then the repeater AP is communicating to computer #2 located 20ft from the repeater AP. The access point unit is located 7.45 miles from computer #1.

### Note

Test Setup A is operation through two repeaters (ham tower unit operates as repeater and so does the one inside the house) and Test Setup B is operation through three repeaters (Sawnee Mtn, ham tower and inside house). In the B setup, an additional repeater access point is inserted in the link between computer #1 and the distant access point. The rest of the physical link is not changed.

To be able to communicate (at all) with the central ham tower site, it was necessary to select “optimize for range” in the express setup screen of the AP342 located at the tower. However, the other two AP342s would operate fine with the “optimize for” selection set to either throughput or range. We made tests with multiple combinations of settings to see what differences were apparent. In addition

to the setup with the two repeaters, we tested setup B (above) which included a direct connection on the 7.5 mile link to the ham tower access point. The data is as follows:

Data transferred consisted of a 2.188-megabyte file. The same file was transmitted multiple times at each setting as we noticed a lot of random (and frequent) speed changes on the 7.45-mile link. Likely this was a result of our location on the mountain where we did not have a clear and direct line of sight path but rather we were looking across the brow of a knoll between the car and the distant ham tower site. I suspect the path had a good bit of multipath. We plan to install a fixed repeater site on this mountain site in the future and we will run the same tests again to see if thing improve when we have a better quality radio link.

The Data: Note: TP=Throughput optimized AP setting, RG=range optimized AP setting

Note: Setup (A) operates through two repeater APs and Setup (B) operates through three repeater APs.

Setup A	Senao/AP	Tower AP Setting	Repeater Setting	Time(s) to Transmit File	Average Throughput
Test 1	Senao	AP=RG	AP=TP	89, 56, 90, 58, 86 sec	288654 bps
Test 1	AP=RG	AP=RG	AP=TP	80, 118, 94, 67, 72 sec	253820 bps
Test 2	AP=RG	AP=RG	AP=TP	65, 74, 82, 78 sec	292709 bps
Test 3	AP=TP	AP=RG	AP=TP	55, 68, 53, 100, 63 sec	322714 bps

The above data is not as high as I had expected. The following are my conclusions at present:

1) The Cisco AP342/AP352 do in fact operate at ranges out to at least 7.45 miles but the data throughput rate is not all that good in the “optimize for range” position. (It may improve when I am able to get a better test position with less multipath.)

2) The throughput does not change greatly if just one AP or multiple APs are placed in range mode and put into operation as repeaters.

3) There has to be a better way to get high-speed data transport using wireless over a wide area using repeaters.

4) The throughput just using the ham tower unit as an AP and accessing the Internet with the AP in range mode was close to full DSL speed. While I do not at present know what the “to be expected” maximum throughput rate for the AP342 used “just as a wide area access point” it appears to be much greater than the speed to be obtained when the AP342/AP352s are used as repeaters in the link.

I will update this data from time to time as more tests are run. One test will be to setup a computer direct to the ham tower AP on the Ethernet side and measure the throughput rate of this “Access

Point Mode” to the remote mountain site. I expect this throughput to be considerably higher. I also will try and locate a better test site with less multipath. But. The wind and temperature on the mountain keeps me mostly in the car!

Here is a quotation from an engineer at Cisco about the AP342/AP352 (specifically) used for longer-range work.

“The ‘optimize for range’ or ‘optimize for throughput’ setting changes the data rates settings for both basic and data rates as well as ‘slot times’. What ‘range’ actually does is to allow a drop down in data rate (if necessary all the way to 1Mbps) for both data packets as well as overhead packets. For the ACK timing this will change the hold off ‘slot times’ to compensate for the longer time it takes for lower data rate packets to get through. This will permit the beacons and other packets, required for maintaining association, to get through easier on the long distance paths.

You got throughput out to 7.45 miles? That’s great. But how many clients were being used at any one time, and what type of traffic load did you have on the AP at the time? We have tested to over 5 miles, but when we started loading up the AP with traffic, we noticed packet retries (on the RF link)

starting to rise rapidly.

So we have still classified the units as 1 mile capability, based on 11Mb and 25 users, pushing 5Mb of traffic (aggregate) through the AP. Keep in mind Cisco is targeting the enterprise and carpeted office, as well as verticals such as Healthcare, Education and retail for the majority of our products and focus. For public access we target hospitality (like hotels) and hotspots (Starbucks, McDonalds, airports) so we have not put any large efforts into longer range public access applications. Hence the lack of features required for the longer ranges.”

Some Operational Observations Of A Cisco Based Network With A BR352 As The Central Node And Five AP342/352s Operating As Repeater APs

1) LinkSys WET11 model 1 units appeared fully compatible with the Cisco gear in all modes. WET11 version 2 units are compatible with the Cisco AP/BR 352/342 units but only if you just use a single SSID. If you use multiple SSIDs in the Cisco gear, WET11 model 2s (with firmware 2.07 and lower) will not associate with the secondary SSIDs. (I am told that version 2.07 supposedly does associate with the primary SSID.)

2) The option to “search for a less congested radio channel” is a nice feature in the wireless setup. I originally fixed my network on channel 5. Six months after installation, I had interference to my system on channel 5 that virtually made throughput from the central bridge go near zero at times. After identifying the problem, I set the central bridge to

allow roaming to channels 3, 4, and 5 if necessary to find a better channel. The system immediately moved to channel 3. Within 10 seconds or so, all of the repeater APs had automatically reassociated and quickly thereafter all of the WET11s had reassociated and were working. Some client cards (Cisco and Orinoco) automatically reassociated while others required exiting the browser and other programs and/or rebooting the computer. The system has stayed on channel 3 and worked fine ever since.

**Table Of Cisco AP352/AP342/BR352 Signal Strength Readings In Percent Converted To dBm**

0%	5	10	15	20	25	30	35	40	45	50	55	60	65	70	75	80	85	90	95	100
-92dbm	-91	-90	-89	-88	-85	-82	-79	-76	-73	-70	-68	-65	-63	-60	-57	-54	-51	-48	-45	-42

3) To read the signal strength from a particular “downstream” remote client radio to AP/BR or from a “downstream” repeater AP to an “upstream AP/bridge or from one repeater AP to the next proceed as follows. (Note: Upstream refers to devices closer to the root AP or bridge device that is connected to the wirelan [usually Internet] interface.) Go to the association table of the AP or repeater AP that is the parent for the particular radio in question. Click on the MAC address for the desired client or other station that claims this AP/repeater AP as “parent” (self in the table). Observe “Latest Signal Strength” in percent in the entry in the right column. This reads the signal strength at the “self” or “parent” of the distant repeater’s signal.

4) To read the signal strength of an “upstream”

root AP/bridge or repeater at a “downstream” repeater, proceed as follows. Go the setup table of the downstream repeater. Look for the network ports line near the bottom of the table. Look to the right for the diagnostics link and click on this link. Click on the radio diagnostics link. Then click on the start button of the antenna alignment test. Wait about a minute and a table of moment-to-moment signal strengths will be displayed.

5) I have not been able to get the carrier test to work on AP342s with firmware version 12.04.

When I try and run a carrier test, the unit is “locked up” for several hours or more and never comes back to life or delivers the channel usage chart. I will try this on an AP352 and BR352 when I get to it.

6) APs have the ability to show traffic to/from the AP in either bytes or packets or both in the association table. (Click on “additional display filters” and set options.) Bridges can only show traffic in Packets. I don’t know if this is a bug in version 12.04 firmware or a limitation of the bridge perhaps running out of memory or CPU capacity.

Does anyone know how the significance of the “signal quality” percentage? If so, please email [joe@mehaffey.us](mailto:joe@mehaffey.us) ###

\*\*Text materials in this paper copyrighted 2003, 2004 by Joe Mehaffey, all rights reserved. Cisco trademarks belong to Cisco Systems.

**Packet Status Register**

#90 Winter 2004, ISSN: 1052-3626

Published by

TAPR  
8987-309 East Tanque Verde Road #337  
Tucson, AZ 95749-9399 USA  
phone 972-671-TAPR (8277)  
fax: 972-671-8716

URL [www.tapr.org](http://www.tapr.org)

TAPR Office Hours

Monday – Thursday, 9 AM – 5 PM Central Time

Entire Contents Copyright © 2003 by TAPR. Unless otherwise indicated, explicit permission is granted to reproduce any materials appearing herein for non-commercial Amateur Radio publications providing that credit is given to both the author and TAPR, along with the TAPR phone number – 972-671-TAPR (8277). Other reproduction is prohibited without written permission from TAPR.

Opinions expressed are those of the authors and not necessarily those of TAPR, the TAPR Board of Directors, TAPR Officers, or the Editor. Acceptance of advertising does not constitute endorsement by TAPR, of the products advertised.

Postmaster: Send address changes to TAPR, P. O. Box 852754, Richardson, TX 75085-2754. *Packet Status Register* is published quarterly by TAPR, 8987-309 East Tanque Verde Road #337, Tucson, Arizona 95749-9399 USA. Membership in TAPR, which supports the electronic publication of the *Packet Status Register*, is \$20.00 per year payable in US funds.

## TAPR is a community that provides leadership and resources to radio amateurs for the purpose of advancing the radio art.

**Submission Guidelines**

TAPR is always interested in receiving information and articles for publication. If you have an idea for an article you would like to see, or you or someone you know is doing something that would interest TAPR, please contact the editor ([wallou@tapr.org](mailto:wallou@tapr.org)) so that your work can be shared with the Amateur Radio community. If you feel uncomfortable or otherwise unable to write an article yourself, please contact the editor for assistance. Preferred format for articles is plain ASCII text (Microsoft Word is acceptable). Preferred graphic formats are PS/EPS/TIFF (diagrams, black and white photographs), or TIFF/JPEG/GIF (color photographs). Please submit graphics at a minimum of 300 DPI.

**Production / Distribution:**

*Packet Status Register* is exported as Adobe Acrobat version 5 and distributed electronically at [www.tapr.org](http://www.tapr.org)

PSR *Packet Status Register* Editor:

Stan Horzepa, WA1LOU  
One Glen Avenue, Wolcott, CT 06716-1442 USA  
phone 203-879-1348  
e-mail [wallou@tapr.org](mailto:wallou@tapr.org)

**TAPR Officers:**

President: John Ackermann, N8UR, [n8ur@tapr.org](mailto:n8ur@tapr.org)  
Vice President: Steve Bible, N7HPR, [n7hpr@tapr.org](mailto:n7hpr@tapr.org)  
Secretary: Stan Horzepa, WA1LOU, 2005, [wallou@tapr.org](mailto:wallou@tapr.org)  
Treasurer: Tom Holmes, N8ZM,, [n8zm@tapr.org](mailto:n8zm@tapr.org)

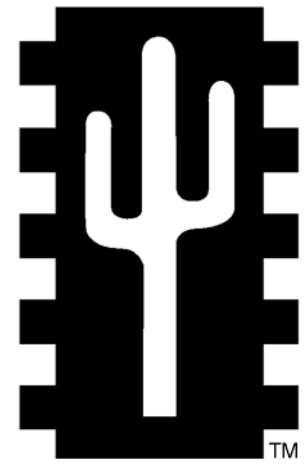
**TAPR Board of Directors:**

Board Member, Call Sign, Term Expires, e-mail address  
John Ackermann, N8UR, 2004, [n8ur@tapr.org](mailto:n8ur@tapr.org)  
Steve Bible, N7HPR, 2005, [n7hpr@tapr.org](mailto:n7hpr@tapr.org)  
Byon Garrabrant, N6BG, 2004, [n6bg@tapr.org](mailto:n6bg@tapr.org)  
Stan Horzepa, WA1LOU, 2005, [wallou@tapr.org](mailto:wallou@tapr.org)  
John Koster, W9DDD, 2006, [w9ddd@tapr.org](mailto:w9ddd@tapr.org)  
Doug McKinney, KC3RL, 2004, [kc3rl@tapr.org](mailto:kc3rl@tapr.org)  
Darryl Smith, VK2TDS, 2005, [vk2tds@tapr.org](mailto:vk2tds@tapr.org)  
Steve Stroh, N8GNJ, 2006, [n8gnj@tapr.org](mailto:n8gnj@tapr.org)  
Brad Noblet, WA8WDQ, 2006, [wa8wdq@tapr.org](mailto:wa8wdq@tapr.org)

TAPR is a not-for-profit scientific research and development corporation [Section 501(c)(3) of the US tax code]. Contributions are deductible to the extent allowed by US tax laws. TAPR is chartered in the State of Arizona for the purpose of designing and developing new systems for digital radio communication in the Amateur Radio Service, and for disseminating information required, during, and obtained from such research.



TAPR MEMBERSHIP	Price	Member Price	Qty	Total	Kit Code
New		\$20.00			0
Renewal, Enter Membership Number here:		\$20.00			0
<b>KITS</b>					
DSP-10 2-Meter Transceiver	\$329.00	\$299.00			56
KK7P DSPx DSP Module	\$99.00	\$99.00			16
KK7P DSP10 Adapter Kit	\$39.00	\$39.00			16
PIC-E(ncoder)	\$65.00	\$58.50			16
Motorola EVM56002 Interface	\$150.00	\$135.00			16
Compact FlashCard Adapter (FlashCard not included)	\$49.00	\$39.00			16
Differential GPS (requires a GPS receiver to operate)	\$199.00	\$179.00			16
DAS (DTMF Accessory Squelch) (as seen in December 1995 QST )	\$68.00	\$61.20			8
TAPR 9600 bit/s Modem	\$80.00	\$72.00			8
Bit Regenerator (for regenerative repeater operation)	\$10.00	\$9.00			1
Clock Option (for regenerative repeater operation)	\$5.00	\$4.50			1
PK-232 Modem Disconnect (to simplify external modem connection)	\$20.00	\$18.00			2
PK-232MBX Installation Kit (for 9600-bit/s modem installation)	\$20.00	\$18.00			2
XR2211 DCD Modification	\$20.00	\$18.00			2
State Machine DCD Modification	\$20.00	\$18.00			2
State Machine DCD Modification with Internal Clock (for KPC-2)	\$25.00	\$22.50			2
<b>FIRMWARE</b>					
TNC2 Version 1.1.9 with KISS EPROM (includes command booklet)	\$15.00	\$13.50			4
TNC2 Version 1.1.9 command booklet	\$8.00	\$7.20			2
TNC2 WA8DED EPROM (ARES/Data standard 8-connection version)	\$12.00	\$10.80			2
TNC1 WA8DED EPROM	\$12.00	\$10.80			2
TNC2 KISS EPROM	\$12.00	\$10.80			2
TNC1 KISS EPROM	\$12.00	\$10.80			2
PK-87 WA8DED EPROM	\$12.00	\$10.80			2
TrackBox EPROM	\$15.00	\$15.00			2
MX-614 Modem IC	\$8.00	\$8.00			2
<b>PUBLICATIONS</b>					
Digital Communications Conference (DCC) Proceedings					
2002 DCC No. 21 (printed copy)	\$20.00	\$18.00			8
2001 DCC No. 20 (printed copy)	\$10.00	\$9.00			8
2000 DCC No. 19 (printed copy)	\$15.00	\$13.50			8
1999 DCC No. 18 (printed copy)	\$15.00	\$13.50			8
1998-2000 DCC Nos. 17-19 (CD & available printed copies)	\$50.00	\$45.00			4
1998-2000 DCC Nos. 17-19 (CD only)	\$33.00	\$30.00			4
1992-1997 DCC Nos. 11-16 (CD & available printed copies)	\$33.00	\$30.00			4
1981-1991 DCC Nos. 1-10 (CD & available printed copies)	\$33.00	\$30.00			4
Earlier DCC Proceedings (printed copies):					
Circle desired nos.: 1-4 5 6 7 8 9	\$6.00 ea.	\$5.40 ea.			8
Circle desired nos.: 10 11 12 13 14 15 16 17	\$6.00 ea.	\$5.40 ea.			8
TAPR Spread Spectrum Update	\$18.00	\$15.30			16
TAPR Software Library CD	\$20.00	\$18.00			4
Wireless Digital Communications	\$39.99	\$36.00			28
Packet Radio: What? Why? How?	\$12.00	\$10.80			8
BBS SYSOP Guide	\$9.00	\$8.10			8
Packet Status Register Vo. 1 (Nos. 1-17, 1982-85)	\$20.00	\$18.00			16
Packet Status Register Vo. 2 (Nos. 18-36, 1986-89)	\$20.00	\$18.00			16
Packet Status Register Vo. 3 (Nos. 37-52, 1990-93)	\$20.00	\$18.00			16
Packet Status Register Vo. 4 (Nos. 53-68, 1993-97)	\$35.00	\$31.50			16
<b>OTHER</b>					
TAPR Badge with Name and Call Sign	\$10.00	\$10.00			0
TAPR 11-oz. Coffee Mug	\$11.00	\$10.00			4
TAPR Shirt (go to www.tapr.org for details)					
<b>GPS EQUIPMENT</b>					
TAC-32 Software Registration	\$55.00	\$55.00			0
Garmin GPS-25 with Data Cable	\$150.00	\$135.00			28
Garmin GPS-20/25 Interface/Power Kit	\$40.00	\$36.00			8
Garmin GPS-20/25 Data Cable	\$15.00	\$15.00			2
Garmin GA-27 GPS Antenna (w/MCX conn., mag. & suction mounts)	\$75.00	\$67.50			8
Oncore UT+ GPS	\$169.00	\$149.00			28
Oncore VP Interface/Power Kit	\$40.00	\$36.00			8
Oncore GT+ GPS	\$149.00	\$129.00			28
Motorola Antenna 97 (w/BNC connector and magnetic mount)	\$65.00	\$58.50			8
MCX Right-Angle Connector with Coaxial Pigtail	\$15.00	\$15.00			2



# TAPR Order Form

**TAPR Business Office**  
**P.O. Box 852754**  
**Richardson, TX 75085-2754**

**Phone (972) 671-8277**

**Fax (972) 671-8716**

**Internet [tapr@tapr.org](mailto:tapr@tapr.org)**  
**[www.tapr.org](http://www.tapr.org)**

Subtotal

Sales Tax (Texas residents only, 8.25%)

Shipping

Total Order Amount

1-7 Kit Code Points: \$6.00  
8-15 Kit Code Points: \$7.00  
16-27 Kit Code Points: \$8.00  
28-55 Kit Code Points: \$9.00  
55 or more Points, contact TAPR

Name \_\_\_\_\_  
Call Sign \_\_\_\_\_  
Street Address \_\_\_\_\_  
City - State - ZIP Code \_\_\_\_\_  
Country \_\_\_\_\_  
Phone Number \_\_\_\_\_  
E-mail Address \_\_\_\_\_

Check Enclosed  or Charge My Credit Card: VISA  MasterCard   
Account Number \_\_\_\_\_  
Expiration Date \_\_\_\_\_  
Signature \_\_\_\_\_