PACKET STATUS REGISTER

Tucson Amateur Packet Radio Corporation

October 1991

Issue # 44

Published by:
Tucson Amateur Packet Radio
PO Box 12925
Tucson, AZ 85732-2925
Phone: 602-749-9479
FAX: 602-749-5636
Office Hours:
Tuesday - Friday
10:00am - 3:00pm M.S.T.

Editor:
Bob Hansen, N2GDE
PO Box 1902
Elmira, NY 14902-1902
CompuServe: 71121,1007

In This Issue...

President's Corner

by Bob Nielsen, W6SWE

METCON-1 is taking off quite well as a kit. The "alpha" boards have all been sold and the TAPR office has received many orders for the production kits. At the time this was being written, parts were arriving, last minute software changes were being checked out, and the documentation was being updated. Hopefully, by the time you read this the back orders will have all been filled. For those with alpha boards who have the capability to re-program the on-board memory in the microprocessor chips, the updated software is available on CompuServe's HAM-NET, or on disk from the TAPR office ($2.00, including postage). The production run has the new software hard coded. These chips are NOT reprogrammable.

There have been a few changes in the TAPR organization. Jerry Crawford, K7UPD, has taken over as Secretary/Treasurer for Greg Jones, WD5IVD, who will be in England furthering his education. Also, Greg Eubank, KL7EV, has volunteered to take over the software library and has some neat ideas for it, which should be in effect by the next issue of *PSR*.

It's time for nominations for the TAPR Board of Directors again. There are five openings for three-year terms on the Board, beginning with the 1992 Annual Meeting. If you would like to submit a nomination (including your own) please see the article elsewhere in this issue of *PSR*. Some of the current directors have indicated that they will not seek re-election, so if you feel that you can contribute to the operation of TAPR, I encourage you to consider this opportunity. Ballots will appear in the January, 1992 issue.

Speaking of the Annual Meeting, the 1992 meeting will mark the tenth anniversary of Tucson Amateur Packet Radio. We are planning to make this meeting "something special," and are soliciting ideas for ways to make this happen. If any of you have suggestions, please let me know either through CompuServe at 71540,2364 or via the TAPR office. I hope that as many members as possible will be able to attend.

TAPR's 10TH Anniversary and Annual Meeting

Yes, it's true; TAPR is 10 years old. To celebrate, TAPR would like to do something special at the upcoming Annual Meeting. If you have any "packet nostalgia" that you would like to share with your fellow packeteers, please let us know. This could include photographs of early packet groups, stories of packet trials and tribulations, early TNCs, or what-have-you. Even if you don't plan to attend the meeting, we would like to hear from you.

The Annual Meeting will be held on March 7-8, 1992, at the Best Western Inn at the Airport, in Tucson, Arizona. The special room rate for attendees is $55 per room, single or double occupancy.

Be sure to mark your calendar and plan to attend. More details will be published in the January issue.

PSR Available for the Blind

The *Packet Status Register* is now available on disk, for visually impaired Amateurs who are interested in packet radio. Please contact the office for more information.

TAPR Board of Directors Election

Tucson Amateur Packet Radio is incorporated in the State of Arizona as a non-profit scientific and educational institution. It is recognized by the IRS as a 501(c)3 tax-exempt organization for these same purposes.

TAPR is governed by a 15 member Board of Directors. Each member of the Board serves a three year term, hence there are 5 positions to be filled each year. Board members are expected to attend the annual Board Meeting, normally held in Tucson in conjunction with the annual TAPR Membership Meeting. They participate in the decision-making process and provide guidance to the officers. They receive no pay and must defray their own expenses to attend meetings. Board members should be prepared to be active in the continuing board deliberations, which are conducted privately in a special conference section on CompuServe. Active participation in TAPR activities by board members is important to the furtherance of the objectives of TAPR. The officers of TAPR are elected by members of the Board at the annual Board of Directors meeting.

The current members of the Board of Directors and the expiration date of their terms are:

Franklin Antonio, N6NKF	1992 *
Tom Clark, W3IWI	1993
Jerry Crawford, K7UPJ	1994
Pete Eaton, WB9FLW	1993
Andy Freeborn, N0CCZ	1994
Bdale Garbee, N3EUA	1992 *
Steve Goode, K9NG	1992 *
Eric Gustafson, N7CL	1992 *
Lyle Johnson, WA7GXD	1992 *
Greg Jones, WD5IVD	1994
Don Lemley, N4PCR	1993
Dan Morrison, KV7B	1994
Bob Nielsen, W6SWE	1994
Harold Price, NK6K	1993
Dave Toth, VE3GYQ	1993

Nominations are now open for the seats expiring in February 1992 (marked with an asterisk).

To place a person in nomination, please remember that he or she must be a member of TAPR. Confirm that the individual is willing to have their name placed in nomination. Send that person's name (your own if you wish to nominate yourself) along with your and their calls, telephone numbers and addresses. The person nominated should submit a short biographical sketch to be published along with the ballot.

Nominations and biographical sketches should be submitted to the TAPR office no later than 1 December 1991.

Ballots will accompany the January issue of PSR or will be mailed directly to the membership. Results will be announced at the annual TAPR Membership Meeting in February 1992.

Packet Status Register (ISSN 1052-3626, USPS 005-419) is published quarterly by the Tucson Amateur Packet Radio Corporation, 9991 E. Morrill Way, Tucson, AZ 85749-9568. Membership in Tucson Amateur Packet Radio, including a subscription to *Packet Status Register*, is $15.00 per year in the U.S. and possessions, of which $12.00 is allocated to *Packet Status Register*. $18.00 in Canada and Mexico and $25.00 elsewhere, payable in U.S. funds. Membership and *Packet Status Register* cannot be separated. Second-class postage paid at Tucson, AZ.

POSTMASTER: Send address changes to *PACKET STATUS REGISTER*, P.O.Box 12925, Tucson, AZ 85732-2925.

DSP Update

by Lyle Johnson, WA7GXD

The DSP project is moving ahead, slowly.

A number of quirks and bugs in the hardware have been revealed as the software folks crank up and begin to port some applications to the board. Development tools are likewise evolving and being ported to the DSP-1.

I'm just as anxious as you are to see this device on the air doing interesting things. But, an amazing amount of work is involved in a project of this magnitude and, with volunteers as the technical staff, things take longer than any of us would like.

Still, there is progress!

I'm Not a Candidate

By Lyle Johnson, WA7GXD

My term on the TAPR Board will expire in February, 1992.

And, I will not be running for re-election.

This decision is motivated by two factors: job and tenure.

Job

My employer, Modular Mining Systems, makes a computer-aided dispatching system used in open-pit and underground mines the world over, to control mining operations. The system uses packet radio techniques to accomplish some of its tasks. (For those of you who haven't been with TAPR since the early days, our first system was installed in 1980, well before TAPR's founding, and does not use a packet protocol even remotely resembling AX.25. TAPR "rose from the slab" in Modular's lab in late 1981.)

This past spring, Modular decided to develop and market some industrial-strength data communications devices very similar to an Amateur TNC. These devices use proprietary protocols and are not AX.25 compatible. There are a number of prototype units in the field undergoing testing as I write this, and the product will be "launched" in a few months.

Ethically, there could be a conflict-of-interest perceived if I were to remain on the TAPR Board once this product is released. TNC manufacturers have an open conduit to the TAPR board and often share information which is not always Amateur-related. If I were to remain on the board, this flow of information might cease or at least be altered. This could harm TAPR and the good work that TAPR does. I do not wish to hinder TAPR's operations in any way.

Tenure

I am co-founder of TAPR and have been on the TAPR Board since its inception. I have served you as an officer for most of the past ten years. I have enjoyed the opportunity to serve you, and I count it a privilege to have been on the Board with some of the best minds and most dedicated people that I know of in the Amateur radio community.

But, ten years is a long time. It is time for new blood and fresh ideas.

Conclusion

Thus, I think it best that I not remain on the board and will not seek another term. I ask you that read this, to seriously consider how you might serve, and if you find it in yourself to want to really give, run for a seat on the Board.

Final-Final

Oh yes, I am still active in technical projects and hope to remain so. You aren't going to get rid of me completely!

Cheers,
Lyle

METCON-1: A Status Report

by Lyle V. Johnson, WA7GXD

METCON is now out of ALPHA test and into production!

One hundred (100) METCON kits were delivered during ALPHA test and we have had feedback from a number of folks about it. As a result of the feedback, the manuals have been extensively revised and the firmware significantly enhanced. METCON-1 kits are now shipping from stock.

Manuals

The voltage-to-frequency (V-to-F) converter documentation has been condensed into a single manual. ALPHA-specific notes have been removed and the manual reflects the temperature option. Detailed procedures for setting up the V-to-F board are now included in the manual.

The METCON assembly manual has been revised and now includes a detailed, step-by-step checkout procedure to ensure everything is working properly before you are sent off to the system manual.

The METCON System Manual has been updated and corrected. It is now sixty (60) pages in length, with details on each and every command and command-bit in the memory map. Each command also has an example showing its use. The memory maps are corrected as well.

Firmware

The new firmware is release 910907-1.02 and includes an enhanced security feature, and a new pulse counter mode, as well as numerous bug fixes.

Security

The old 6-digit password access has been supplemented by a "no security" option as well as an "authentication security" mode.

No security means that no password of any type is needed. This is handy for checkout on your PC before installing the unit in a remote site.

Authentication security involves METCON issuing you a three digit challenge, to which you must respond with data from a large table that METCON will generate for you. This is similar to the NET/ROM system, but uses a much larger table and is all hex encoded.

Pulse Counter

One user requested a pulse counter rather than a frequency counter mode for the binary inputs. His specific application was for a rain gauge for a remote weather site. Each of the METCON binary inputs can now be configured by command to operate as a frequency counter or a pulse counter.

Other Details

In order to keep costs down, the microcomputer used in the production boards is not re-programmable. This means that if a new release of firmware is developed and you desire to use its features, you must buy a new chip. The cost for a new chip should remain well below $20, pre-programmed.

Alpha owners may update their firmware to the latest by sending their 87C51 microcomputer chip to the TAPR office. Send it in a protective carton and plugged into anti-static foam. We'll re-program the chip and send it back to you for $5 postpaid and include the new manual as well.

If you've been looking for a good, non-text application for packet radio, METCON is for you!

Deviation Meter

by Lyle Johnson, WA7GXD

On Friday, September 20th, the first prototype bare PC boards for the new TAPR Deviation Meter were delivered to the TAPR office. (I am writing this on Sunday the 22nd and no, I don't have one built and running yet!)

Overview

The prototype boards measure 3" by 5" and are complete.

The deviation meter (DevMtr) consists of a synthesized 2-meter receiver, a calibration oscillator, a microprocessor, a four-digit numeric display, three switches, an RS-232 serial port and a power connector!

Why Do We Need This?

Correct deviation settings are important for best operation of your packet station. Over-deviation (which is pretty common) results in retries or even not getting through with a rock-crushing signal. Under-deviation is less of a problem. Deviation settings are one case where less is more.

Unfortunately, reasonably accurate deviation measuring equipment is very expensive and unavailable to most hams.

How Will It Work?

There will be a couple of modes of operation.

The basic mode will be to turn on the DevMtr and then key up your 2-meter transmitter. Put your TNC in CAL mode if you can, or just send a few frames otherwise -- but keep the transmitter keyed! After a number of seconds, the DevMtr will find you, center on your signal and report your deviation on the built-in display.

The second mode will be for you to key in your transmit frequency so the DevMtr won't have to search for you. Then, whenever it hears a signal above a certain strength, it will report deviation to you.

Simple, eh?

What About High-Speed Packet?

High speed on 2-meters is limited by bandwidth and regulatory considerations. Nonetheless, the DevMtr will be able to handle signals of around 30 kHz to maybe 100 kHz in bandwidth. The details remain to be worked out, but the receiver uses commercial FM broadcast filters so a 100 kHz wide signal can easily pass.

What Will I Need To Set It Up?

Just a terminal and power supply. The terminal (or computer) will let you command the DevMtr to measure specific voltages while you make adjustments.

The DevMtr includes a synthesized calibration oscillator that sweeps the IF of the receiver. The microprocessor measures the voltage from the FM detector and saves this as a calibration curve (so the detector doesn't even have to be very linear), then compares this to your signal. If your signal falls below a limit, the DevMtr will re-calibrate over a narrower range. If your signal exceeds a limit, the DevMtr will re-calibrate over a wider range.

How Accurate Will It Be?

The goal is to get you within two percent.

What About A Case?

The 3" by 5" size means that cases are available at your local grocery store in the form of under-a-dollar recipe boxes! Just don't get a metal one since the receiving antenna is etched on the PC board...

How Much Will It Cost?

The TAPR Board directed me to keep it as cheap as practical. My personal goal is to have the kit able to be sold for under $100. Preliminary cost estimates tell me this should be possible. But, you never know until the prototype is working and that isn't the case yet...

When Will It Be Available?

This is a toughie. I want it done yesterday. A realistic goal is to have the prototype running before year's end. I would like to see kits released at the 1992 TAPR Annual Meeting.

And, I am terrible at making accurate predictions of this sort...

An Introduction to Packet Satellites

by Jonathan Naylor, G4KLX

[Reprinted from the August 1991 (Number 90) Oscar News, published by AMSAT-UK]

Background

Packet radio has been used on Amateur satellites since the early 1980's. The first to exploit the mode was UoSAT OSCAR 11 which was constructed by the University of Surrey and launched in early 1984. Experience gained from this and other satellites has evolved to the current generation of packet satellites known as PACSATs.

A complete list of Amateur satellites that have used packet radio is given below:

UO-11

Launched in 1984. This satellite uses a form of packet radio for its Digital Communications Experiment (DCE) used to pass packet mail around the world. It is only accessible via official ground stations so that access to the DCE is via your local mailbox. Non-standard AFSK is used on 2m and 70cm. Still active.

FO-12

First Japanese Amateur satellite, launched in 1986. Was the first open access packet satellite available to suitably equipped ground stations. Its uplink was on 2m and downlink on 70cm (Mode J). It used a modulation technique called Phase Shift Keying (PSK). FO-12 also carried a linear (i.e. SSB, CW) transponder. FO-12 was switched off in late 1989 due to failing batteries.

AO-13

The second phase-3 Amateur satellite. It carries a system called RUDAK which would have provided world wide coverage for long periods of the day. Unfortunately RUDAK never operated correctly and is now abandoned. AO-13 itself is fully operational and is providing superb non-packet communications.

UO-14

First PACSAT. Built by the University of Surrey and launched along with the next five satellites in January 1990. Its mailbox is called the Packet Communications Experiment (PCE) and is the testing ground for all the new ideas that the new packet satellites use. It is a MODE J system and uses the G3RUH 9600 baud modem design that allows a vast amount of data to be transferred in a short time. Still active.

UO-15

Built by the University of Surrey. It carried a high performance camera and was going to use the 9600 baud system to send images down to Earth. It failed in orbit one day after launch for reasons unknown.

AO-16

Is similar to UO-14 in concept and internal design. It uses the same modulation system as FO-12 (PSK) and therefore its data rate is only 1200 baud. Built by AMSAT-NA. Still active.

DO-17

Built by AMSAT-NA and sponsored by Junior, PY2BJO. Its primary aim is to be an educational tool, its eventual aim is to "speak" its data. Its downlink is on 2m and uses conventional packet radio for its telemetry. Still active.

WO-18

Built by AMSAT-NA and sponsored by Weber State University in Utah. Its aims were similar to UO-15 but uses the slower PO-12 PSK system for downloading its data. Still active.

LO-19

Built by AMSAT-NA and sponsored by AMSAT-LU. Is very similar to AO-16. Still active.

FO-20

Second Japanese Amateur satellite. It is a carbon copy of FO-12 although it carries more solar cells and has a new aerial design. It was launched in February 1990. Still active.

AO-21

A joint Russian/German satellite. It is a passenger on a Russian navigation satellite. The packet radio side is called RUDAK-2 and is truly amazing in its capabilities. It uses Digital Signal Processing (DSP) and is therefore capable of supporting any existing or future modulation techniques. It was launched in early 1991. Still active.

UoSAT-F

This satellite is to be launched on 8th May 1991. It is a cross between UO-14 and UO-15. The mailbox operation is on non-Amateur frequencies for third world relief operations. The camera on-board will transmit on the same frequency as UO-15 used, and will have a resolution of better than 2km.

The satellites of most interest are UO-14, AO-16, LO-19, and UoSAT-F. My reason for believing this is that the techniques are more advanced than the other satellites, and they represent the true tradition of Amateur radio. The mailbox on-board FO-20 is very similar to the ones in use on Earth and is, by definition, not very efficient. This last statement needs some explanation.

The Problems of Satellite Packet Radio

If a satellite carrying packet radio flies over a heavily populated area, a number of problems occur. These problems are caused because the satellite can "see" a large ground area (e.g.: the whole of Europe, half of America, whole of Japan) and will therefore be within the range of a potentially large number of users. If all of these Amateurs log into the satellite at the same time, the system would fail. Most satellites have a limit on the number of simultaneous users, and on any given pass, only a small percentage of users will be able to use the satellite (usually those with the largest amplifiers).

Another problem is that the satellite is only available at a given location for a number of short time periods during the day. These time periods can range from one to twenty minutes long. Even during a satellite pass, the signal may become weak and drop out due to natural phenomena. It is essential that any system devised should allow for breaks during the transmission and reception of data to and from the satellite. The ground station should be able to continue with its task after a delay of many hours, or even days.

Satellites use full duplex operation, therefore the transmitting ground station does not listen to its own transmit frequency. Even if it were, it would not make much difference: an Amateur in the UK would not hear a ground station in Germany on 70cm, for example, because each would have his beam aimed at the satellite. The satellite would hear both signals, and others, resulting in QRM and reduced efficiency. One solution to this problem is to have multiple uplink frequencies. This technique is used on all of the satellites in an attempt to ease this problem.

The more radical solution, dreamt up by the designers of these new satellites, is very simple, but requires a completely new point of view. The solution is to try and reduce the number of transmissions needed by a ground station to read mail. They reasoned that most mail is made up of bulletins that are read by a large proportion of the users. Therefore they devised a Broadcast Protocol that allows the satellite to transmit bulletins of general interest at all times. Each one of these transmissions has enough identification within it to allow it to be slotted into a message without reference to any previous transmission. The ground station may transmit to ask the satellite to put a particular message onto the broadcast schedule for a particular period of time.

The problem with this idea is that it assumes that the ground station has some sort of computer available to process incoming data into a usable form. This is not an entirely unreasonable assumption to make since inexpensive computers are now prevalent. It is definitely not possible to use a dumb terminal with one of the new PACSATs.

Renew Your Membership!

TAPR doesn't send out constant reminders when your membership has expired. Our only way of communicating your expiration date to you, is the date on the address label for this issue. Please check it and renew if required. Your membership is very important.

Setting up a Station - Radio

The RF side of a PACSAT station is not too demanding on an Amateur who is moderately well equipped. All of the packet satellites described above, except AO-21, use Mode J. This involves a 2m uplink with a 70cm downlink; AO-21 uses Mode B, which is 70cm uplink and 2m downlink. My comments from now on are specifically for operating Mode J.

The antennas required to work these satellites do not need to be big. A large aerial may be quite a liability as it will need adjusting often to track the satellite as it crosses the sky. It should be remembered that once the satellite is above ten degrees of elevation, then the path between the satellite and your ground station is essentially line-of-sight. Large antennas are not needed. Aerials as simple as crossed dipoles and two turn helicals may be used, and they require no tracking at all. I use a six element beam on 70cm (the back of a 21 element Tonna) with a permanent tilt of 30 degrees, for my PACSAT work.

A pre-amplifier is generally not needed. The signals are strong, but if your receiver is poor, or your feedline is lossy, or your antenna gain is low, then a cheap pre-amp mounted at the antenna will be advantageous.

Once you get to the radios, some choices need to be made. The choice depends on whether you are going to use PSK on AO-16, LO-19, and FO-20, or the 9600 baud system on UO-14 and UoSAT-F.

The transmitter should be FM. Ideally you should be able to apply your transmit audio to the modulating element directly. This is because the filtering of some radios can seriously distort the transmitted audio, and make it unusable. This is certainly true of the 9600 baud system, the 1200 baud PSK system benefits from no filtering and can usually pass through most radios.

The radios needed for the reception of the different satellites are fundamentally different. For 1200 baud PSK on AO-16, LO-19, and FO-20, any 70cm SSB receiver with up/down microphone controls is suitable. The Yaesu FT790R is ideal in this role and is now quite cheap. For UO-14 and UoSAT-F, an FM receiver is needed; ideally it should have AFC to track the doppler shift present on the signal. The University of Surrey uses modified Wood & Douglas strips, unfortunately, I don't have details of the modifications. The FM receiver should be modified so that the audio can be tapped off from just after the demodulator to avoid any audio filtering. A modified FT790R can be used in this role.

Setting up the Station - Digital

The audio from the radio must be fed into a suitable demodulator. The standard modem in a TNC is not suitable for this use and will have to be bypassed; most TNCs have a modem disconnect header for this purpose. The new modem required depends on which satellite group you plan to use. For UO-14 and UoSAT-F a G3RUH 9600 baud modem needs to be used. You can build one yourself quite easily, alternatively you can buy special TNCs such as the Kantronics Data Engine with DE-9600 mode, or the Pac-Comm TINY-9600, a high speed version of the TINY-2.

For the other satellites a PSK modem is required. G3RUH also designed one of the definitive designs for this format. There are two commercial PSK modems available at the present time, one is the Pac-Comm PSK-1, and the other is made by Tasco. *[Editor's note: The Pac-Comm PSK-1 is a licensed variation of the TAPR PSK modem.]*

The TNC itself should be operating in KISS mode. In this mode, the TNC does a bare minimum of processing and passes the data, almost raw, through to the computer attached to its serial port. Most TNCs have KISS mode built-in. It is recommended that the speed of the serial port be greater than the speed of the data coming down from the satellite. For example, 2400 baud for 1200 baud PSK system, and 19200 baud for the 9600 baud system. Note that some TNCs cannot operate at the higher speeds, most notably the Kantronics line prior to the Data Engine.

As mentioned above, a computer is essential in order to use these new satellites. It is a fact that the PC compatibles are the predominant type in use today, and it is not a coincidence that the processors used in these new satellites is from the same family as those used in the PC compatibles.

The software needed to use these new satellites is available from a number of sources, and for a number of different computer families. The University of Surrey published specifications for the new protocols early on, and it gave independent developers time to write their own implementations. The "official" University of Surrey software is public domain and contains two parts: PB to access the Broadcast protocol, and PG to allow uploading of files and more complex tasks. There are a number of utilities also available for manipulating telemetry such as activity logs and the like. These are all for PC compatibles only.

Problems

No system is perfect and satellites are no exception. A number of Amateur satellites have failed to operate correctly once in orbit, most notably UO-15. Due to their complexity, the PACSATs have only started to be usable since December 1990. Even at this stage, the PACSAT software occasionally crashes and the ground controllers have to take remedial action to prevent it from happening again. FO-20 is also having difficulties caused by its particular orbit; since the middle of 1990, FO-20 has been in constant sunlight, causing its internal temperature to rise to almost 50 degrees C. This may cause the batteries of the satellite to fail prematurely.

Operating Mode J may cause problems due to desensitization fo the receiver by the third harmonic of the transmitter. This can usually be cured by including filters in the aerial leads for both the transmitter and receiver.

Doppler shift is a problem when using all satellites in a low orbit, such as the PACSATs. Most of the satellites referred to here travel at around 7 km/s around the Earth, the resultant Doppler shift at 145 MHz is +/- 3 KHz and at 435 MHz it is +/- 10KHz. The PSK modems designed for AO-16 etc. produce signals which control the up/down lines on modern synthesized radios. On satellites that use FM, such as UO-14, the modem cannot produce a similar signal, however, AFC is easy to achieve on an FM radio.

Frequencies

Here is a list of the frequencies in use by the currently active packet satellites:

UO-11
Downlink: 145.825 MHz

UO-14
Downlink: 435.070 MHz
Uplinks: 145.975, 145.900 MHz

AO-16
Downlink: 437.025 MHz
Uplinks: 145.900, 145.920, 145.940, 145.960 MHz

DO-17
Downlink: 145.825 MHz

WO-18
Downlink: 437.075

LO-19
Downlink: 437.150 MHz
Uplinks: 145,840, 145,860, 145,880, 145,900 MHz

FO-20
Downlink: 435.910 MHz
Uplinks: 145.850, 145,870, 145,890, 145.910 MHz

AO-21
Downlink: 145.983 MHz
Uplinks: 435.016, 435.155, 435.193, 435.041 MHz

Unlike the other satellites, the uplink frequencies for AO-21 have different modems attached to them. The downlink frequency is also capable of carrying different data formats, including CW and normal FM speech. AO-21 is a very complex satellite and further reading is recommended before attempting to use it.

AO-16, DO-17, WO-18, and LO-19 all have alternate transmitters that are activated on Experimenters Day, which is usually every Wednesday. These transmitters also operate on 70cm, and are usually 50 KHz away from the frequencies listed above. AO-16 and DO-17 each carry a transmitter on 2.4 GHz which is switched on occasionally; LO-19 has a separate transmitter on 437.125 MHz which transmits telemetry in CW.

10th ARRL Computer Networking Conference Report

by Lyle Johnson, WA7GXD

This year's conference was held in San Jose, California, the weekend of September 28th and 29th. I drove from Tucson so I missed the Friday sessions, but heard about them from others.

This year's conference was organized a bit differently than previous ones.

There were pay-to-attend tutorial sessions on DSP and Spread Spectrum held on Friday afternoon. Friday evening included a Luau and ended with 'til midnight "birds of a feather" (BOF) gatherings, where folks could sit around and chat with others about specific areas of Amateur digital communications.

Only eight (8) presenters showed up, so each talk had an allotment of about 45 minutes. This is much more time than has been available at previous conferences. However, the Proceedings ($12 from ARRL) have twenty two (22) papers filling 164 pages and is well worth the price.

K3MC started off with a talk on using a full-duplex CSMA/CD approach to 56 kbps packet operation using the WA4DSY modem.

N6GN followed with an update on the Hubmaster system, including 903 MHz radios and a high-speed PC-bus digital interface card. The Northern California Packet Association has a number of these transceivers in beta test, and they look very interesting for point-to-point work. The hubmaster concept is simply to have a central station serving the various users, much like a repeater serves a group of users. This way, folks can operate at high data rates with directional antennas and get better overall operation.

VE4WK then spoke about methods that can be used for data compression, including simple approaches that can yield around 40% improvement for "normal" text applications.

KA9Q rounded out the morning with a different approach to measuring spectral efficiency, taking into account the geographic area that is impacted by a given transmission.

After lunch, VE3FZK gave an entertaining talk about using doppler-based direction finding gear linked by packet to rapidly locate the bad guys so the good guys can intervene.

VE4WK returned with a talk about real-time speech compression using DSP technology. His group has succeeded in making a system that gives good quality speech at 4800 bps.

W7GHM then gave a technical overview of the Clover-2 HF data communications system he has been designing for the past several years. This is a DSP-based box that give 31.25 to 750 bps throughput on HF channels in a 500 Hz bandwidth. Several prototypes are running.

WU2N wrapped up the session with a talk on the use of Graphical User Interfaces (GUI) for packet applications. His example was a callsign server that ran on both MacIntosh and MS-DOS running Windows 3.0.

A banquet followed with a speech by an FCC staffer talking about spectrum efficiency. A lot of questions were asked afterwards, not always with soft voices...

BOF sessions followed, with the Clover-2 demonstration room being quite crowded (I didn't make it to any others -- I was just too fascinated by this one!).

Sunday morning the ARRL digital committee met and discussed a few topics including the new makeup of the committee after 1991. The committee will be dissolved and two committees created -- one will deal with operational issues of the existing digital scene, the other long-range planning and implementation. The 11th Conference may be held in New Jersey. The AX.25 V2.1 spec is long overdue and I volunteered to try and get it done.

There were parallel sessions for beginners at no charge.

Besides TAPR, vendors present at the conference included HAL, Kantronics, and Pac-Comm. Missing were AEA, Gracilis, and MFJ.

There were 131 pre-registered attendees.

BBS Message Authentication

by Phil Karn, KA9Q

[This letter is reprinted from the July 1991 issue of QEX, published by the ARRL.]

I've had several requests for the "white paper" on cryptographic authentication of BBS messages that I wrote recently in response to a query by Paul Rinaldo, W4RI, of the ARRL. Paul is the chairman of the ARRL Digital Committee, of which I am a member.

In case anybody can't tell, the opinions expressed here are my own.

- Phil Karn, KA9Q

Paul,

This is in response to your request to the Digital Committee for comments on authentication schemes that might be used to verify the source and integrity of a message posted to an Amateur BBS network. This letter consists of a quick tutorial on the various forms of cryptographic authentication, some personal judgements about their practicality and suitability for the problem at hand, and some personal opinions on the present regulatory situation.

The scheme that I talked about at the 1987 ARRL Networking Conference was for authenticating IP datagrams using DES, but the same principles apply to using any conventional secret key cipher to authenticate any kind of message. (By "authenticate a message," I mean verifying that the message was, in fact, sent by the claimed sender, and that the message contents have not been modified along the way.) Such schemes require all the stations involved, to share a single secret key. Without the key, you cannot compute the proper authenticator for the messages you send, nor can you verify an authenticator received with an incoming message.

The difficulty of key management with a conventional cipher can range from "trivial" to "intractable," depending on the application. Key management is simple as long as there are only a few stations that need to generate or authenticate messages, and all trust each other. For example, a DES-based scheme could be applied to a repeater to limit remote control to a few trusted stations. A single key known to the repeater would be shared by the control stations and kept secret from everyone else. An in-person meeting of the telephone would suffice for distributing the DES keys.

Now consider cases where the operators do not necessarily trust each other, e.g., autopatch operation. Since many more stations use an autopatch than control the basic operation of the repeater, its owners may want individual accountability. A DES-based authentication system could still work if each user has his or her own key. The same system could be used to control access to a BBS. In either case, the "server" (the repeater or BBS) keeps a complete list of keys for all authorized users, and logs each access. This is more work than the previous case, but it is still entirely practical.

Common to all these schemes so far is the assumption that only the server needs to authenticate a request, e.g., the repeater controller or the BBS. It must protect its users' keys against unauthorized disclosure, but since the resource being protected by the authentication system is the server itself, the owner of the server has an incentive to do this.

But, in the more general case where individual pairs of stations must be able to authenticate each other, things get much more complicated. Each pair has to have a key that is known only to that pair; if you have N stations, you need a total on N^2 keys. All these keys must be exchanged by some secure means before authentication can occur, and they must be kept secret. To do this for every pair of Amateurs in the world is clearly impractical. And, if you want **any** Amateur to be able to verify the authenticity of, say, a "broadcast" BBS message (to carry on the Amateur "self-policing" tradition, of course), there is **no** solution using conventional cryptography -- the same key needed to verify a message could be used to forge one.

Some form of secret key authentication might still be practical between neighbors in a packet backbone or a BBS auto-forwarding network. But this would authenticate only your immediate neighbors; it would not authenticate the origins of the traffic they pass from other nodes. For example, one BBS SYSOP could create illegal traffic and then pass it to a neighbor claiming that it originated somewhere else, and there would be no way to disprove this. So you really do want the authentication to be "end to end," not "hop by hop," so we are left with an unsolved key management problem.

One way to reduce the N^2 key problem is to establish a "key distribution center" that maintains a list of all the users' private keys. Users wishing to authenticate themselves to each other do so by first authenticating themselves to the key distribution center (KDC). The KDC then generates a "session key" (a random number) and sends it to the two parties encrypted in their own keys. The parties then decrypt the session key, yielding a shared secret that can be used for authentication. Still, only the parties involved can authenticate each other; someone listening in could not. (In most environments, this is an advantage; somebody else's conversations are none of your business.)

MIT has developed a system based on this model called "Kerberos." It is in operation at MIT and elsewhere (the code is free). Nevertheless, it has the drawback that authentication depends on the availability and reachability of the KDC. But the fact that the KDC must have a complete list of the users' private keys works against deploying multiple KDCs with copies of the database for redundancy; the more KDCs there are, the more opportunities for the database to be compromised. The scheme also assumes that all of the parties (the two users and the KDC) have the ability to communicate with each other in real-time, a bad assumption for Amateur packet radio.

So the inescapable conclusion is that authentication schemes based solely on private key cryptography are of limited utility in Amateur packet radio; they cannot solve the general problem. Fortunately, there is a new alternative: public key cryptography (PKC). in PKC, the keys used for encryption and decryption are different. Furthermore, knowledge of the encryption key, K_e, does not imply knowledge of the decryption key, K_d; in fact, the algorithms ensure that it is extremely difficult to determine K_d from K_e. The combination of K_e and its corresponding K_d is call a "key pair;" for this reason, public key crypto-systems are sometimes called "dual key" ciphers, as opposed to "single key" ciphers like DES.

The leading public key scheme, RSA, was invented by Ron Rivest, Adi Shamir, and Len Adelman while at MIT. They hold a U.S. patent on it that is being exploited by RSA Data Security, Inc. (There is no patent protection on RSA outside the U.S.)

The original idea behind RSA was to allow you to publish K_e (hence the name, "public key" cryptography) so anyone could send you a secret message without prior arrangement. As long as you keep K_d secret, only you can decrypt it. But when used "backwards," RSA can also do authentication. If you encrypt a message using K_d (your decryption key, known only to you), then anyone can decrypt it using your K_e (your public encryption key). Anyone who decrypts such a message then knows that whoever generated it must have known your K_d. This procedure of using RSA in reverse is called "signing."

In practice, it is not desirable to run an entire message through RSA to authenticate it because it is very slow, much slower than secret key ciphers like DES. There is a better way. Functions exist to quickly "hash" a message of arbitrary length into a relatively small, fixed size "message digest." They are much like cyclic redundancy codes (CRCs) except that they are much more complex because they are designed to detect intentional "transmission errors" as well as natural ones. With a good function, it is computationally infeasible, even for someone who knows it, to produce two message that hash to the same value, or to determine the input that produces a given value. They are not ciphers because they have no key and their outputs cannot be "decrypted."

One message digest algorithm is "message digest #4" (MD4) by Ron Rivest, who has placed it in the public domain. MD4 takes a message of any length and produces a 128-bit (16 byte) result. Rivest conjectures that it would take on the order of 2.5^{64} operations to find two inputs that hash to the same value, and 2.5^{128} operations to find an input that hashes to a given value. These are impressive numbers, so if the algorithm holds up under analysis, it should be quite secure in practice.

Given RSA and MD4, one authenticates a message by first computing its hash code (by encryption with the sender's private key, K_d) and the result is appended to the message. The party wishing to authenticate the message also computes the message digest. It then decrypts the encrypted message digest received with the message (using the published key of the sender, K_e) and compares it to the value it has just computed. if they match, the message is genuine.

There stills remains the problem of distributing the public keys. Although they may be freely read by anyone, they must still be protected against modification. Otherwise, someone might forge a signature of a message under someone else's name using a public-key/private-key pair of his own creation. If the receiver can be duped into accepting this bogus key, then he will believe that the signature is genuine.

One way is to publish the public keys as widely as possible in so many places that no one could possibly modify all of the copies of a particular key that reach the intended target of a deception. For example, the keys could be publish on CD-ROM or they could be listed in the back pages of QST. But these schemes have two drawbacks: cost and time.

Another refinement, "certification," addresses this problem. If a "certifying authority" can be set up to sign the public keys of individual users with its private key, then only the public key of the certifying authority needs to be widely published. For example, the ARRL might select and publish its own public key in QST. It could then accept public keys from individual Amateurs (accompanied with some non-cryptographic form of authentication, such as a notarized statement). The ARRL would sign the individual public keys with its private key and return the results. Note that the ARRL need not know the individual's private key.

The signed public keys are known as "certificates." They can be distributed by the users themselves (e.g., in a mail header) because anyone can readily verify their authenticity with the published ARRL public key. This eliminates the need for an on-line KDC. The ARRL's workload might be a problem, but a solution exists for this too: a hierarchy of certifying authorities. For example, each ARRL Division might act as the certifying authority for the Amateurs in its area using a Division public key that has been certified by ARRL Headquarters. Divisions might further delegate the workload to their constituent Sections. The verification of an individual user's certificate would therefore require the certificates of all of the certifying authorities in the hierarchy, as well as, the published key of the ARRL.

So, in theory, authentication based on public key cryptography solves many of the problems associated with the earlier secret key schemes. However, many practical obstacles would still remain:

1. The RSA algorithm is patented in the U.S. and the owners of the patent are holding it fairly close to their chest. Negotiations between RSA and the Internet Activities Board have been dragging on for several years now over an agreement for the use of RSA in the Internet. It is not at all clear how much the patent royalties will be, or how they will be charged. (The leading theory is that the royalties will be tied only to the issuance of certificates, not to the actual implementation or use of RSA, but this is not yet final.) Would the use of RSA in Amateur packet radio (resulting in the payment of royalties to RSA DSI) be considered as furthering the "regular business affairs" of RSA DSI?

2. The algorithms are, by Amateur standards, quite complex. At a minimum, they would probably require every Amateur to have a PC-class computer to hash and sign messages. Given that a major reason TCP/IP is still a relatively esoteric mode in Amateur packet radio is the reluctance of many Amateurs to upgrade from C-64s and

"dumb terminals," it seems unlikely that universal user authentication could happen any time soon. And I won't even begin to discuss the user education issues.

3. Even if a full-blown RSA-based authentication system, as described earlier, could be deployed, it is not clear that it would solve the specific problem that originally prompted your query. Someone accused of posting an illegal message to an Amateur BBS could still claim that his secret key had been stolen and used by someone else. Or, he could accuse the local "Section Certification Manager" of signing a bogus public key with his call sign on it and using it to "frame" him by sending verboten traffic. Even if a key really has been stolen and the owner notifies the certification authorities, how do they spread the word that the previously distributed public key is no longer valid? These issues are still the subject of much discussion in the research community. Furthermore, this technology has yet to have its first real test in a court of law.

In summation, although I find cryptographic authentication to be a fascinating topic that has some potential for use in Amateur Radio, I do not feel that it is "ready for prime-time." Mandating its use at this time would be an enormous over-reaction to the "problem" of controlling inappropriate BBS traffic.

Quite frankly, the FCC's heavy-handed behavior in this case has me greatly concerned. I think they are going after a fly with a battleship. I do not know whether they sincerely believe that they are "protecting" Amateur Radio, or if they have some more sinister motive. I can only hope for the former, so we can reason with them. Every new development carries with it some risk of abuse; the more powerful the technology, the greater the risk. Amateur packet radio is no exception; even in its presently primitive state, it is useful enough to tempt some commercial entities to abuse it. We should be able to convince the FCC that requiring unrealistically stringent mechanisms to prevent even the occasional commercial abuse of Amateur packet radio runs the far greater risk of destroying all of the good that it can do.

Lately, several of us (WA8DZP, K3MC, N6RCE, NG6Q, and I) have been taking a close look at the low-power spread spectrum modems that are rapidly becoming available for use under Part 15 rules on 902-928 MHz and other shared ISM/Amateur bands. In my own opinion, building high-speed (say, 100 to 500 kbit/s) metropolitan area networks under Part 15 rules seems entirely feasible, even with the 1-watt power limit, given proper design and engineering (good sites, directional antennas, power control, efficient channel access methods, etc.). Sure, the performance of the existing generation of equipment is disappointing, mainly due to the lack of receiver processing gain in most models. But with the new FCC rules mandating the use of "true" spread spectrum receivers, plus the commercial drive behind this industry, it seems likely that the cost/performance ratio of this equipment will rapidly improve. Unfortunately, the same probably cannot be said for Amateur packet radio gear, where the large scale production of inexpensive, high speed radio modems seems as far away as ever. Hence our initial interest in this technology.

But this latest blow from the FCC is making Part 15's absence of licensing requirements, content and/or usage restrictions look mighty attractive indeed, even though my primary intent is to use the network for the kind of personal experimentation that has traditionally been done in the Amateur service. Are the FCC's rules really "protecting" the Amateur service if they scare off those who are most interested in making technical contributions to the service?

I think it is time that the FCC remove the burden of responsibility for content from automatic relay stations and loosen up its Draconian definition of "business communications." A lot has happened to the telecommunications industry since the Eyebank Docket; in particular, it is certainly no longer the job of the FCC to protect a telephone company from "lost business." The Amateur rules should be pragmatic with the realization that absolute prohibitions do far more harm than good.

A simple "hams shalt not sell communications services" rule should suffice to make any abuses self-limiting because few hams are willing to use their time and their stations to help make money for others, if they don't get a cut of it. Such a rule would be far clearer than the present "no business interest" rule. The current rule has spawned an entire generation of armchair Amateur lawyers who revel in interpreting the rules in the most restrictive fashion possible. To see the chilling effect of the present rules, one only needs to look at how the field of computer networking is pretty much passing Amateur Radio by.

Notes from the TAPR Office

by Heather Johnson, N7DZU

Efficiency and Quality; things we strive for!

Unfortunately, we have had some unusual things happen to our disk-duplicating machine in the past few months. First, the motherboard died. Next, one of the disk drives died, then the power supply, then one of those ring protectors that are around the center of each disk decided to remain INSIDE of the machine getting in the way of the spinning action of the disks...

Another problem has been with the badges. It has been difficult to keep them looking uniform, as each time I make another order they return either with thinner printing, or the numerals have been mistaken for letters... (Ever try and explain the difference between a "zero" and on 'oh' to a non-ham?) We are working on these problems, so keep the badge orders coming!

Lyle and I enjoyed attending the ARRL Networking Conference last weekend (September 28 & 29). While there, I met a gentleman, Mike Curtis, who offered to help us with something that I have felt we needed. He says that if you will send him an SASE and TWO copies of your radio schematic, he will mark one to show you where you hook up your 9600 baud modem to it. Thank you, Mike!

You may reach Mike at this address:

Mike Curtis
7921 Wilkinson Ave.
North Hollywood, CA 91605

Until next issue, 73
Heather

PSK Use on 10 Meters

[The following items appeared in the May 1990 and September 1990 issues of QEX, published by the ARRL.]

HF Packet Radio with PSK Successful

by Julius W. Breit, W9UWE, and Walt Kaelin, KB6BT

Early in 1990, Walt Kaelin, KB6BT, and Julius Breit, W9UWE, got several multi-mode TNCs that have phase-shift keying (PSK) modulation. Out of curiosity, they decided to try PSK rather than FSK on HF packet radio. Since early February of that year, they have been operating 1200 baud PSK on 10 meters, and the results have been astonishing.

Both stations are using TASCO TNC-24 MK II TNCs and Kenwood TS-440S tranceivers, with power outputs of 50 watts into vertical antennas. They are 4000 km apart. Much of the time, their HF PSK circuits compare very favorably with 1200 baud VHF/UHF PSK operation. If a "half-way decent" transmission path exists between them, they have no problem transferring lengthy files in approximately the same amount of time it takes on the landline at 1200 baud.

S-meter readings above S-1.5 at KB6BT and W9UWE will usually provide an immediate connect. Signals between S-1.5 and S-2 will pass traffic with mediocre results, usually with repeats. Signals above S-2 give excellent results with very few repeats. They also can handle traffic under severe fading conditions. The 1200 baud speed is fast enough to send one or more packets and receive an acknowledgment during signal peaks. They have set their PACLEN to 40 and have turned on CONPERM to prevent disconnection during fading.

PSK shows a surprising immunity to noise. At times, when the signal seems barely audible in the noise, the stations will connect and acknowledge.

KB6BT and W9UWE believe that they are the first hams in the U.S. to use PSK on HF. If any readers have PSK HF capability, Walt and Julius invite you to connect to them and leave a message. Presently, they are operating on 28.119 MHz USB. W9UWE is on the air most of the daylight hours with the mailbox callsign of W9UWE-1, while KB6BT is on the air 24 hours per day, using the mailbox callsign of KB6BT-7.

The FCC restricts 1200 baud operation to 10 meters and above, but if you search, you can find much 1200 baud PSK activity on 15 meters when the band is open to the Pacific area. Many hams in Japan, Philippines, and Australia have switched to PSK operation, and you can find them on 21.105 and 21.109 MHz LSB.

KB6BT and W9UWE like their results and are enthusiastic about the possibilities and advantages of PSK versus FSK HF packet radio. Give PSK a try to see if it can be the solution for some of our HF packet radio problems.

More PSK Activity

by John A. Mezak, K2RDX

On September 10, 1990, John Mezak, K2DRX, in San Jose, California, contacted Julius Breit, W9UWE, in Chicago via 1200 baud PSK packet radio on 10 meters. John was very surprised at the throughput using PSK under very marginal conditions. John and Julius were able to chat keybaord to keybaord even though they had no S-meter readings, and 10 meters was closing down. John used a TAPR PSK modem with an MFJ-1274 TNC, ICOM IC-751A, and a J-pole vertical antenna.

The results on 10 meters were so good that K2RDX started sending CQ packet beacons through OSCAR 13 on mode B. The majority of his beacon packets were demodulated and correctly received on the downlink frequency. Even mode L signals were consistently coming through, despite 10 dB S/N ratio (maximum) at his receiver (from his own transmit signal). On the OSCARs, John used an FT-736R at 25 watts on 435 MHz and 40 watts on 1269 MHz with an external power amplifier. Considering the length of time OSCAR 13 is visible, John believes a considerable amount of traffic could be handled by a few PSK packet radio stations during an emergency, without requiring much satellite transponder power.

[Editor's note: Also of interest on this topic, is an article in the July 1991 issue of QEX by John Reed, W6IOJ, describing a PSK demodulator designed specifically for narrow-band applications.]

Software Library Update

by Bob Nielsen, W6SWE

Here are the current versions of all the disks in the TAPR software library, as of September 23, 1991. Among the updates is a new version of the KA9Q NET version of tcp/ip software, provided by Joe Buswell, K5JB. Joe has enhanced the ax.25 mailbox and condensed the code to the point where the executables and source will both fit on two diskettes. Thus disk 12/12A is no longer part of the listing. We have also added two new disks. Disk 32 is PAMS, a Personal AMTOR Mailbox SYSTEM by W5SMM and disk 33 is a Z-80 monitor for the TNC-2 and clones by AD7I.

Revisions since the last issue are indicated by an asterisk (*) above. Where a double entry is shown (i.e., 11/11A), two disks are required in 5-1/4 in. DSDD format (1 disk in 3-1/2 in. format). TAPR attempts to supply the latest version of all software, however we cannot distribute what we do not have. Authors are invited to send updates to their software (and new offerings) to the TAPR office. The office can provide disks and mailers for updates upon request.

Disk No.	Name	Version	Date
1.	APLINK	VER. 5.05	07-05-91*
2.	AA4RE BBS	VER. 2.11	03-06-91
3.	CBBS	VER. 6.6	03-09-90
4.	EZPAC	VER. 1.1	01-09-89
5.	MONAX		10-30-87
6.	PACKET_SHARE		08-22-90
7.	W9ZRX BBS LIST		04-24-89
8.	R95		09-01-89
9.	ROSERVER PRMBS	VER. 1.55	07-31-91*
10.	ROSE SWITCH	VER. 901111	11-15-90
11/11A	KA9Q NET	VER. K5JB.J64	08-20-91*
13.	TNC1 CODE		05-30-84
14.	TNC2 NOTES		03-28-90
15.	WA7MBL BBS	VER. 5.14	02-11-90
16.	WRLI BBS	VER. 13.00	05-08-91
17.	YAPP	VER. 2.0	12-18-86
18/18A	INTRO TO TCP/IP		09-09-87
19.	LAN-LINK	VER. 1.59	03-27-91*
20.	ARESDATA	VER. 1.5	01-20-91
21/21A	MSYS	VER. 1.11	04-04-91
22.	G8BPQ NODE	VER. 4.04	07-31-91*
23.	UTILITIES		
	PKARC	VER. 3.6	06-01-88
	PKZIP	VER. 1.10EX	03-15-90
	LHA	VER. 2.13	07-20-91*
	ZOO	VER. 2.01	08-25-88
24.	THS	VER. 2.50	11-11-89
25.	VE4UB NTS	VER. 012891	01-28-91
26.	NM1D DOSGATE	VER. 1.14	11-29-89
27.	SV7AIZ BBS	VER. 3.24	04-05-90
28.	TEXNET	VER. 1.6	02-05-91
29.	INTRO TO PACKET RADIO		11-04-90
30.	MICROSAT GROUND-STATION SOFTWARE		
	PB		05-09-91*
	PG		02-12-91*
	PFHADD		12-21-90
	PHS		12-21-90
31/31A	KA9Q NOS	VER. G1EMM 1.6	01-19-91
32.	PAMS-Personal AMTOR Mailbox	Ver. 1.03	09-23-91*
33.	TNC-2 Z-80 Monitor	Ver. 2.00	09-02-91*

Membership Application

TAPR is a non-profit, volunteer operated Amateur Radio organization. Membership in TAPR, including a subscription to *Packet Status Register*, the TAPR newsletter, is $15 per year in the U.S. and possessions, $18 in Canada and Mexico, and $25 elsewhere, payable in U.S. funds only. VISA and Mastercard accepted. Membership and *PSR* subscription cannot be seperated. $12 of the dues is allocated to *Packet Status Register*.

Name:		New:
Address:		Renewal:
City:	State:	
Country:	Zip:	Check:
Call Sign:		Credit Card:

VISA / MasterCard only			Expiration Date:		
Card Number					
Signature:					

The Tucson Amateur Packet Radio Corporation is a non-profit, scientific research and development corporation. TAPR is chartered in the State of Arizona for the purpose of designing and developing new systems for packet radio communication in the Amateur Radio Service, and for freely disseminating information required during, and obtained from, such research.

The officers of the Tucson Amateur Packet Radio Corp. are:

Bob Nielsen, W6SWE	President
Harold Price, NK6K	Vice President
Jerry Crawford, K7UPJ	Secretary/Treasurer

TAPR Membership and
***PSR* Subscription Mailing Address:**
Tucson Amateur Packet Radio Corp.
PO Box 12925
Tucson, AZ 85732-2925
Phone: 602-749-9479
FAX: 602-749-5636
Office Hours: Tuesday - Friday
10:00am - 3:00pm M.S.T.

***PSR* Editorial (Only) Address:**
Bob Hansen, N2GDE
PSR Editor
P.O. Box 1902
Elmira, N.Y. 14902-1902
CompuServe: 71121,1007

TAPR Board of Directors

Board Member	Term	CompuServe
Antonio, Franklin N6NKF,	1992	76337,1365
Clark, Tom W3IWI,	1993	71260,3640
Crawford, Jerry K7UPJ, *	1994	70521,2356
Eaton, Pete WB9FLW,	1993	72727,2641
Freeborn, Andy N0CCZ, *	1994	73177,1317
Garbee, Bdale N3EUA,	1992	76430,3323
Goode, Steve K9NG,	1992	70525,364
Gustafson, Eric N7CL,	1992	71750,2133
Johnson, Lyle WA7GXD, *	1992	76246,565
Jones, Greg WD5IVD,	1994	72047,3455
Lemley, Don N4PCR,	1993	73230,310
Morrison, Dan KV7B,	1994	70541,2374
Nielsen, Bob W6SWE, *	1994	71540,2364
Price, Harold NK6K, *	1993	71635,1174
Toth, Dave VE3GYQ,	1993	72255,152

Date is expiration of term on Board of Directors.
Asterisk indicates member of Executive Committee.

The TAPR Board of Director members "attend" a meeting, which is continuously in session, in a reserved area on the CompuServe information network. The Board encourages input from all interested members. If you have an issue you want addressed, or an idea for a project you would like TAPR to sponsor, contact any Board member, or drop a note to the TAPR office.

To send E-mail to a CompuServe account from the Internet, use the address:
`XXXXX.XXXX@compuserve.com`
where the X's are the CompuServe ID number. Note: be sure to use a period, not a comma, in the ID number.

Packet Status Register
Tucson Amateur Packet Radio Corp.
PO Box 12925
Tucson, AZ 85732-2925

SECOND CLASS
POSTAGE PAID AT
TUCSON, AZ.

PACKET STATUS REGISTER

ISSUE #44

October 1991

Check your address label for membership expiration date. Your renewal is important!