NCPA Downlink

The Official Journal of the Northern California Packet Association
Serving Amateur Radio Digital Communication in Northern California

Summer, 1991 | **Issue number 7** | **Price: $3.50**

Increasing Your Baud Rate

Larry Kenney, WB9LOZ
NCPA Education Coordinator

There are several ways to increase your baud rate without actually changing from 1200 baud to 2400 or 9600 baud. Let's take a look. They're all important things to remember that will help increase your throughput and make your time spent on packet more rewarding and enjoyable. (Throughput is a word that has come into use by packet operators and means the amount of usable packet information sent or received by a station.)

Looking for Information

One of the ways to increase your baud rate is to know where to look for information. There are two main sources on a packet bulletin board system: messages and files. Here are some of the differences between these two forms:

MESSAGES are numbered in the order received, which makes it easy to check the latest news. Just read the largest message numbers. Unlike files, messages can be sent personally to another ham and can travel to other BBSs. Bulletins are automatically killed after a week or so, so they could be called the BBS's news wire.

FILES are the library of the BBS. The files are organized into several directories so all of the files dealing with a topic are grouped together. The files are all available for all users (unlike personal messages). Files cannot automatically be sent from one BBS to another like messages can, so much of the file material originally came in as messages. Because of the way files are grouped, it is much easier to find the information you want from the files section of the BBS, than it would be to look through hundreds of messages. Unlike messages, files do not get killed after a week or so. If the information is relevant, they may stick around for months, maybe years.

The 10th ARRL Computer Networking Conference is coming to San Jose September 27-29!
See page 3 for details.

You just might want to take a look to see what's in the library at your BBS. You might be amazed at the information you'll find. Enter a W for a listing of the various directories and then search the ones where you think you'd find the information you desire. Some examples are: packet tutorials to help make packet operating easier for you, BBS and node lists, information on using the node network, the ARRL and RACES Bulletins, AMSAT information, technical hints, rig modifications, callsign data, FCC exam locations, the FCC Rules and Regulations - Part 97, NTS message and traffic handling instructions, weather data, TCP/IP information, and maybe even software programs.

Due to the limits of DOS, the operating system used on most BBSs, file names are limited to 11 characters, eight before the dot, three after it. With these limitations, it's often difficult to name the files so that the user can easily identify the information. You might have to study the file names a bit to figure out what they're about.

Operating Hints

Whether you're making local keyboard to keyboard QSOs, checking into a BBS or mailbox, or working DX, here are a some facts you should take into consideration that will help eliminate problems and waiting time and will increase your throughput.

When connecting to another station, don't use a digipeater or node unless you have to. Each digipeater you add to the path increases the time required to get your signal to its destination and to get an acknowledgement returned. It also increases the chance for interference and for collisions with other packets. You'll be amazed at the difference in throughput

Continued on page 4

In This Issue

Where to Find a BBS

N0ARY-1	Sunnyvale	144.93
KE6BX	Hollister	144.93
KJ6FY-1	Benicia	144.93
KI6YK	Danville	144.93
WD6CMU	Richmond	144.97
N6EEG	Berkeley	144.97
W6FGC-2	Twain Harte	144.97
K6LY	Monterey	144.97
N6LDL	Los Gatos	144.97, 145.71[1]
KI6WE	Pleasant Hill	144.97
KD6XZ-1	Sacramento	144.97, 441.50
AA4RE-1	Gilroy	144.99
KA6FUB	Martinez	144.99, 441.50
N6OA	Lemoore	144.99
W6PW-3	San Francisco	144.99
WA6RDH	Dixon	145.01, 441.50
KG6EE	Santa Cruz	145.07
KI6EH	Santa Cruz	145.07
N6IIU-1	Palo Alto	145.07, 223.56
AL7IN	Rohnert Park	145.07
KE6LW-1	Yuba City	145.07, 441.50
KG6XX-1	Carmichael	145.07, 441.50
W6CUS-1	Richmond	145.09
N6ECP	Redding	145.09
KB6IRS	Soquel	145.09
N6IYA-2	Felton	145.09
K3MC	Fremont	145.09, 145.75[2]
WA6NWE-1	North Highlands	145.09, 441.50, 144.93[2]
K6RAU-1	Merced	145.09
WA6YHJ-1	Livermore	145.09
W8GEC	Boulder Creek	145.73
WA6HAM	Pittsburg	145.73
KB5IC	San Jose	145.73
KA6JLT-2	Menlo Park	145.73, 145.71[1]
N6MPW	Ben Lomond	144.79
WB6ODZ-1	Lake Isabella	145.79
N6QMY-1	Fremont	145.79, 441.50
N6REB-2	Modesto	145.79

[1]9600 baud port
[2]TCP/IP port

The NCPA *Downlink*

Editor:
Steve Harding, KA6ETB
BBS: KA6ETB @ N6LDL.#NOCAL.CA.USA.NA
Internet: steveh@arasmith.com

Assistant Editor:
Larry Kenney, WB9LOZ
BBS: WB9LOZ @ W6PW.#NOCAL.CA.USA.NA

Layout/Typesetting:
Eric Williams, WD6CMU
BBS: WD6CMU @ WD6CMU.#NOCAL.CA.USA.NA
CompuServe: 71336,1424
Internet: wetleric@cca.ucsf.edu

Printing:
Glenn Tenney, AA6ER
Internet: tenney@well.sf.ca.us

Staff:
Mike Chepponis, K3MC
BBS: K3MC@K3MC.#NOCAL.CA.USA.NA
TCP/IP: mike@k3mc.ampr.org
Internet: mac@leg.ai.mit.edu
CompuServe: 72117,2732

Patrick Mulrooney, N6QMY
BBS: N6QMY @ N6QMY.#NOCAL.CA.USA.NA
Internet: pat@ub.com

The NCPA *Downlink* is published quarterly by the Northern California Packet Association, 6680B Alhambra Ave. Suite 111, Martinez, CA 94553, for the entertainment and education of amateur Radio operators using digital modes, and those with an interest in them. A one-year membership in the NCPA, including a subscription to the NCPA *Downlink*, is $10.00 per year in the U.S. and its possessions.

10th ARRL Amateur Radio-Computer Networking Conference

27-29 September 1991, Radisson Airport Hotel, San Jose, CA

The Northern California Packet Association (NCPA) is hosting this year's ARRL Computer Networking Conference and invites you to attend. Glenn Tenney, AA6ER, is the local conference chairperson.

Hams from around the world will be presenting papers on what they're working on in "packet radio". The presentations and papers may cover subjects from satellites to spread spectrum, from protocols to hardware, or any other topic related to how hams are, or will be networking.

In addition to the usual presentation of papers all day Saturday, this year's conference will be surrounded by other interesting and informative activities.

AGENDA

Friday, 27 September

13:00 — 17:00: In-Depth Tutorials (special event)

Three concurrent in-depth technical sessions:

- Digital Signal Processing
- Spread Spectrum and Part 15
- Packet Satellites

The speakers are currently working on the leading edge of these technologies. Subjects will be covered in depth, right down to the bits and bytes level.

Cost: $30/person, $40 after August 20th

19:00 — 21:30: Dinner (special event)

Instead of everyone trying to find a pizza joint....we've decided to have a very special group dinner. You can join everyone for a LUAU! Yes, a real honest to goodness luau! This should be an ideal time for everyone to relax. Plan to join us, even if you aren't attending the tutorials. This will be right at the hotel.

Cost: $35/person, $40 after August 20th

Saturday, 28 September

08:30 — 17:00: Presentation of CNC Papers

This is the traditional part of the conference.

Cost: $30/person, $40 after August 20th (includes printed copy of proceedings and lunch)

18:30 — 21:00: Dinner (special event)

The CNC doesn't stop at dinner. We will have an important guest speaker at this banquet. You won't want to miss this!

Cost: $30/person, $40 after August 30th

21:00 — 24:00: Birds of a Feather sessions

Ten or fifteen minutes per paper really isn't enough, so we've planned break-out rooms for "Birds Of a Feather" sessions. During the day we'll have sign-up sheets so that discussion groups can form and really get into topics of greatest interest.

Sunday, 29 September

As usual, the digital committee will have their business meeting Sunday morning from 09:00 until 12:00. But that's not all...

We're going to have a demo room available from about 09:00 until 13:00. We're hoping that you'll be able to bring a rig with you to show off your latest work. We may also have some exhibitors.

But wait, that's still not all...

We're going to present various newcomer tutorials from 10:00 until 13:00. These tutorials may be for the first-time packet user, while others may be for the first-time TCP/IP user. These tutorials will help folks learn more about various aspects of packet radio. The demo/exhibit room and newcomer tutorials will be open to all hams and prospective hams whether signed up for the rest of the conference or not.

And finally, the San Jose Technology Center is a short light-rail ride away and they have a fantastic high-tech museum called The Garage. Although a trip to the Garage isn't an official part of the CNC, we're sure a large group will be planning to visit it on Sunday.

For more information, contact:

Glenn Tenney, AA6ER
Fantasia Systems Inc.
211 Ensenada Way
San Mateo, CA 94403

Voice: (415) 574-3420
Fax: (415) 574-0546
Internet: tenney@well.sf.ca.us
Compuserve: 70641,23

Plan now to attend the conference, Friday through Sunday, September 27-29.

Increasing Your Baud Rate

Continued from page 1

when comparing a direct connect to one with just one digipeater in the path.

The packet node network does a great deal to help you get your packets through, but you must remember that throughput there, too, is affected by the number of nodes and the conditions between you and the destination station. The big advantage of the nodes is that the acknowledgements do not have to return all the way from the destination station. Packets are acknowledged from node to node, so that eliminates a large part of the problems encountered. Getting the original packet through, however, remains to be as much of a problem for the nodes as it is for you when using digipeaters. It can take several minutes to get a packet through when you're working a station some distance away.

If you have a choice, use a frequency that doesn't have a lot of other traffic on it. It makes sense that the more stations there are on frequency, the more chances there are for collisions and retries. A path that will work perfectly without a lot of traffic, can become totally useless under heavy traffic conditions. Just one additional station on the frequency can decrease throughput by about half in many cases.

Another consideration, especially if working over a long distance, is atmospheric conditions. You might not have experienced this before on VHF, but with packet's high sensitivity to noise, a slight change in signal strength can mean the difference between getting your packets through or not getting them through. The mid-day heat in the Central Valley can have a very noticable negative affect on signal strength, causing paths to disappear. In the Bay Area the fog has a drastic affect on signals. When a fog bank is moving in off the Pacific, it can act as an excellent reflector. Signals that are not normally heard can reach signal strengths of 40 over S9.

Multipath is another problem that can greatly affect your packet signal. Multipath is the term used to describe the reception of multiple signals from one source due to reflections off of buildings, hills, mountains or fog. The ghost in a television picture is a form of multipath. A station with a very strong signal into a digipeater or node often cannot use that path if multipath causes the signal to be distorted. Each packet is checked for 100% accuracy and is not acknowledged unless it is. Multipath reflection can cause occasional bits to be lost so you end up with multiple retries and a poor path even with strong signals.

If you use packet on HF, remember to change your transmit baud rate to 300. You will also need to make some other changes, because on HF you don't get a nice clean path like you get on VHF. QRM, QRN, fading, and multipath are ever present on the low bands. To compensate, use a short PACLEN (a value of 40 seems to work quite well) and a MAXFRAME of 1. The chances of getting a short packet through the noise and QRM are much better than for a long one.

Message Addressing

This is another area that can help speed up the data flow on packet. When you send a message, the type of message should be indicated by the user, and not left to be determined by the BBS software. You know best what type of message you're sending. The SP command should be used when sending a PERSONAL message, a BULLETIN should be entered with the SB command, and all NTS messages should be entered with ST. Entering only an "S" should never be used when entering a message.

You should also make sure that you enter enough addressing information to get the message to its destination. If the message is being sent to a station at another BBS, be sure you enter the call of the other BBS correctly, and if the message is going to someone outside of Northern California, you need to include the two letter state abbreviation, as a minimum, and the regional code if it's known. Messages going to another country must have the country and continent included. The full address format is:

```
SP CALLSIGN @
 BBS.#REGION.ST.COUNTRY.CON-
 TINENT
```

Here are some examples:

```
SP KC6NVL @ K6VE.#SOCA.CA
SP NG2P @ WB2WXQ.#WNY.NY
SP VE1BUF @ VE1FUN.NB.CAN.NA
SP G4MPQ @ GB7PLY.#44.GBR.EU
SP 7J1ACT @
 7J1AAA.#10.JNET1.JPN.AS
```

You'll note that each part of the address is separated by a period. Regional codes are preceeded by a pound sign (#), and state, country and continent abbreviations must be the standards that have been agreed to. Addressing for stations in other countries might vary somewhat from the standard format, as shown in the last two examples above.

When sending a bulletin, the message should be addressed TO the appropriate category, such as PACKET, KEPS, MOD, SALE, etc., @ the designator for the area desired. These designators are:

ALLCAN: All BBSs in Northern CA

ALLCA: All BBSs in California

ALLUSW: All BBSs in the western US (CA,OR,WA,NV,AZ)

ALLUS: All BBSs across the entire US.

For example:

```
SB PACKET @ ALLCAN
```

Note: Special care should be used when addressing a message @ ALLUS, because the capacity of transcontinental

Editor's note: Recently there has been some controversy over the use of the continental designator, especially the use of .NA for North America. It seems there are several gateway stations transferring messages between the BBSnet and the Internet. (The Internet is a network tie of most commercial, educational, and some personal computer networks.) It seems that a gateway sent BBSnet traffic into the Internet with the .NA continental designator attached. This traffic was promptly sent to Namibia, the owner of the .NA designator on the Internet. This error, which has been resolved, cost Namibia many dollars, as they pay for there Internet feeds, even if the traffic is refused.

Therefore, those of you who have Internet and BBSnet access, be careful of how you sign your messages. Differentiate between your Internet and BBSnet addresses. If you are replying to a message, be sure you are replying to the correct address on the correct net.

AA4RE and W0RLI are aware of the problem, and there has been much discussion on ways to alleviate it.

The Future of Packet...What Will it Bring?

by Travis A. Wise, KB8FOU

Travis is an active 16 year old ham who is working hard to encourage other young people to check out Ham Radio. He operates a Ham radio BBS system called the HAMBBS, 300/1200/2400 (408) 267-6396 which has hundreds of Ham Radio (and packet) files.

With the advent of the new Technician license, we will be seeing an increase in packet users. My packet station is on all the time, and every day I keyboard to new folks who just got their TNC, and some who just got their license. With increased numbers, the load on the BBS network increases, and at the same time, the number of people on any one of the packet frequencies increases.

While packet was designed for many QSOs (whether they be keyboard, BBS, Node, etc.) to take place at the same time, there is an upper limit where the frequency gets clogged, and communications break down. There are many ways to solve this.

First of all, we can stay at 1200 baud and increase the number of frequencies we can use. Okay, 1200 was nice to start with, but it just isn't working any more. Therefore, we need to look at faster speeds. David Singer, N6TFX, gave a very complete (and understandable!) talk and demo at the West Valley Amateur Radio Association March general meeting about high speed packet. From that talk, I learned that while 9600 baud packet sounds fast, it really isn't. I think that an optimum packet network would utilize 9600 baud for the BBS to user connection, but something faster, like 19.2, or better yet, 56kb. The technology is here, it's just a matter of getting it working.

Keep in mind that if the BBSs forward through the backbone at 19.2 or 56kb, and the HF gateways stay at 300, if we hook the system up right, a message could cross the country faster on VHF than HF, which has a lot of potential, as well as problems. Some argue that packet isn't the future of ham radio, but as more people get involved with packet, the volume of traffic increases, and new forms of moving the traffic become necessary.

Another topic which I would like to briefly mention is the recent 900 number situation. I'm not really surprised that we have had a problem like this, considering how long packet has been in existence, and how many users there are. There's bound to be a problem now and then. I don't agree with how the FCC initially handled the situation, and I'm not happy with the end result, that is, most BBS's having to hold all traffic before forwarding for screening, but I guess it shouldn't be much of a surprise. I've heard several people say that the packet network is falling apart, what with the SYSOPS having to screen messages, and with the area designators like "ALLUS" describing nothing like the actual coverage the message carrying that title is getting. I don't think that's the case, though. I think the packet system will recover nicely, with changes in the system (maybe removal of the message header which takes up space and tells the FCC right who they need to 'contact'). I hope so anyhow. EOF

---

circuits is limited. The message should be of wide interest to amateurs in all parts of the country, it should not have a time constraints, and it should be as short as possible. Sale messages should not be sent @ ALLUS, because the item will probably be sold locally before the message ever gets to more distant areas.

So that the person reading your message can respond to you, include your FULL packet address as part of your signature in the text of the message. Unless the person receiving your message has your full address, he might not be able to determine where to send a response back to you. The address for anyone with a home BBS in Northern California is: **(yourcall) @ (BBScall).#NOCAL.CA.USA.NA** For example:

```
WB9LOZ @
 W6PW.#NOCAL.CA.USA.NA
```

Note: The local area is #NOCAL, not #NORCAL or #NOCA, and the state is CA, not CAL or CALIF. Only the two letter state abbreviation is recognized by BBS software.

Receiving Your Messages

Many packet users check into more than one BBS on occasion. BBS DXing is discouraged, but for many users there are two or three local BBSs that can be accessed quite easily. No matter how many systems you check into, you should remember these two very important points:

Use only one BBS as your home BBS. Whenever you have to enter the callsign of your home BBS, always enter the same one.

Make sure you use the call of a full service BBS, one that carries bulletins and is part of the forwarding network.

There are very important reasons for this. The White Pages directory is used very frequently by people to find out where to send messages. If you use different callsigns, the directory information will vary and your messages will be sent to a variety of locations. In addition, some of the BBS software uses this home BBS information to make sure your mail reaches you. It will automatically check the White Pages for the home BBS of the addressee whenever a message reaches its destination. If a message is misaddressed, the software will make a correction and try to send the message to the right system. If you use different home BBS callsigns, your messages can be sent from one BBS to another, then possibly back again, often looping between systems, never reaching a final destination.

If you use the callsign of a TNC mailbox or personal BBS, the forwarding system won't have any idea where to send the message. These calls are not included in the forwarding files of most systems. If you want your mail to come directly into your mailbox, ask your sysop if he can automatically forward it there for you. Many sysops will do this if you agree to leave your mailbox on the BBS frequency during the hours you agree on with the sysop. In this case, you still tell the outside world that your address is the full-service BBS. The mail comes first to the BBS and then directly into your mailbox.

As long as you list the same home BBS callsign every time and use the call of a full service BBS, you can be assured that your messages will reach you.

EOF

Thoughts on BBS Authentication

Phil Karn KA9Q

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.

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 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 contorl stations and kept secret from everyone else. An in-person meeting or the telephone would suffice for distributing the DES keys.

Now consider cases where the operators do not necessarily trust each other, eg, autopatch operation. Since many more stations use an autopatch than control the basic operations 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, eg, 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 of 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 autoforwarding 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 schemes 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, they 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 called a "key pair"; for this reason, public key cryptosystems 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 US patent on it that is being exploited by RSA Data Security, Inc. (There is no patent protection on RSA outside the US.)

The original idea behind RSA was to allow you to publish Ke (hence the name, "public key" cryptography) so anyone could send you a secret message without prior arrangement. As long as you kept 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 reduncancy 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 infeasable, even for someone who knows it, to produce two messages 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^{64} operations to find two inputs that hash to the same value and 2^{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 with MD4. Then RSA is used to "sign" the 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 still 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 public 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 the copies of a particular key that reach the intended target of a deception. For example, they keys could be published 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 keys.

The signed public keys are known as "certificates." They can be distributed by the users themselves (eg, in a mail header) because anyone can redily 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 the ARRL Headquarters. Divisions might further delegate the workload to thei constituent Sections. The verification of an individual user's certificate would therefore require the certificates of all the certifying authorities in the hierarchy, as well as the published key of the ARRL.

So, in theory anyway, 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 US 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

Continued on page 9

Northern California Packet Band Plan

50 MHz

51.12	SOCAL backbone
51.14	Experimental
51.16	Keyboard to Keyboard
51.18	Experimental

144 MHz

144.91	Keyboard to Keyboard
144.93	LAN[1]
144.95	DX Cluster
144.97	LAN
144.99	LAN
145.01	Keyboard to Keyboard
145.03	Keyboard to Keyboard
145.05	Keyboard to Keyboard
145.07	LAN
145.09	LAN
145.71	9600 bps
145.73	LAN
145.75	TCP/IP
145.77	DX Cluster
145.79	LAN
146.58	DX Cluster

[1]Some TCP/IP in Sacramento grandfathered

220 MHz

223.54	Node uplink (East Bay)[1]
223.56	Node uplink (East Bay)
223.58	Node uplink ("Other")[2]
223.60	Node uplink (Sacramento Valley)
223.62	Node uplink (South Bay)
223.64	Node uplink (North Bay)
223.66	Keyboard to Keyboard
223.68	LAN
223.70	Node uplink (Monterey Bay)
223.72	TCP/IP
223.74	DX Backbone

[1]To move to .56 when SOCAL coordinates

[2]TCP/IP interlink (Sacramento) Not to interfere with node uplink.

440 MHz

433.05	TCP/IP Backbone (100 Khz wide)
433.15	NETROM Backbone (100 Khz wide)
433.25	DX Cluster Backbone (100 Khz wide)
433.31	Experimental
433.33	Experimental
433.35	Experimental
433.37	Experimental
433.39	DX Cluster backbone
433.41	BBS Interlink
433.43	9600 Bps
433.45	BBS Interlink
433.47	NETROM Interlink (KB-to-KB)
433.49	TCP/IP
441.50	All

900 MHz

903.500	1 Mhz wide - TCP/IP
904.500	1 Mhz wide - TCP/IP
915.500	1 Mhz wide - Experimental
916.100	200 Khz Wide - Experimental
916.300	200 Khz Wide - Experimental
916.500	200 Khz Wide - Experimental
916.650	100 Khz Wide - Experimental
916.750	100 Khz Wide - Experimental
916.810	20 Khz Wide - Experimental
916.830	20 Khz Wide - Experimental
916.850	20 Khz Wide - Experimental
916.870	20 Khz Wide - Experimental
916.890	20 Khz Wide - Experimental
916.910	20 Khz Wide - Experimental
916.930	20 Khz Wide - Experimental
916.950	20 Khz Wide - Experimental
916.970	20 Khz Wide - Experimental
916.990	20 Khz Wide - BBS links (Contra Costa County only)

900 MHz activity is on a non-interference basis to vehicle locator service. 900 MHz is not considered suitable for omin-directional systems, use for point-to-point links only.

1296 MHz

1248.500	1 Mhz wide - Full duplex with 1299.500 Experimental
1249.000 to 1249.450	Unchannelized - Experimental
1249.500	100 Khz wide - Experimental
1249.600	100 Khz wide - Experimental
1249.700	100 Khz wide - Full duplex with 1299.700 Experimental
1249.800	100 Khz wide - Full duplex with 1299.800 Experimental
1249.870	20 Khz wide - Experimental
1249.890	20 Khz wide - Experimental
1249.910	20 Khz wide - Full duplex with 1299.910 Experimental
1249.930	20 Khz wide - Full duplex with 1299.930 Experimental
1249.950	20 Khz wide - Full duplex with 1299.950 Experimental
1249.970	20 Khz wide - Full duplex with 1299.970 Experimental
1249.990	20 Khz wide - Full duplex with 1299.990 Experimental
1250.500	1 Mhz wide - Experimental
1251.500	1 Mhz wide - Experimental
1297.000 to 1298.000	Unchannelized - Experimental
1298.500	1 Mhz wide - Full duplex with 1299.500
1299.000 to 1299.450	Unchannelized - Experimental
1299.500	100 Khz wide - Experimental
1299.600	100 Khz wide - Experimental
1299.700	100 Khz wide - Full duplex with 1249.700 Experimental
1299.800	100 Khz wide - Full duplex with 1249.800 Experimental
1299.870	20 Khz wide - Experimental
1299.890	20 Khz wide - DX Packet Cluster users
1299.910	20 Khz wide - Full duplex with 1249.910 Experimental
1299.930	20 Khz wide - Full duplex with 1249.930 Experimental
1299.950	20 Khz wide - Full duplex with 1249.950 Experimental
1299.970	20 Khz wide - Full duplex with 1249.970 Experimental
1299.990	20 Khz wide - Full duplex with 1249.990 Experimental

Definitions

Experimental — Anything goes except full service BBS or any 24 Hr/Day services (nodes, gateways, etc). This is where you can come and test new gear, programs, etc. These channels may be reassigned in the near future so no permanent activities please.

Backbone, Uplink, Interlink — No uncoordinated stations. These channels are for specific purposes as defined by the NCPA and affiliated groups. This is where the various BBS, nodes, and clusters interlink and are very high usage channels. Please use the normal 2 meter entry points of the network you want to access rather than these channels.

Keyboard to Keyboard — Anything but full service BBS, TCP/IP, or DX Cluster. Primarily chat channels. These are also the primary emergency channels. Some existing BBS systems (eg. WA6RDH) were grandfathered.

A gray area is "Personal BBS." A PBBS is one with a small number of users (rule-of-thumb: five or less). A PBBS should not be attracting general users thru beacons, etc. Bulletins should be confined to local information and not duplicate the general bulletins send to the community. That's the job of a full service BBS and we have lots of them in Northern California to use.

LAN — Local Area Network. Anything except TCP/IP and DX Cluster is tolerated. Please avoid placing high level digipeaters or nodes on these channels since they are "local." A low-level node that links into a backbone on another frequency is the preferred implementation.

TCP/IP — Stations using TCP/IP protocol on top of AX.25. Some AX.25 tolerated to communicate to TCP/IP stations if p-persistance access method used.

DX Cluster — Northern California DX spotting network. No other activity should be on these channels.

9600 Bps — Stations using 9600 Bps with direct FSK (G3RUH, TAPR, etc.) modems.

Procedure for changes

Users should contact either the frequency coordinator or the NCPA board. The frequency coordinator will then present the requests to the board at the next meeting along with suggested assignments. The NCPA board elected by you, the packet user, makes all assignments!

Electronic mail is preferred.

Note: NCPA does not coordinate individual stations, nodes, etc. The only station coordination is done by K6RAU for bulletin board systems.

EOF

Thoughts on BBS Authentication

Continued from page 7

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 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 it is "ready for prime-time." Mandating its use at this time would be an enormous overreaction 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 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 902-928MHz and other shared ISM/amateur bands. In my own opinion, building high-speed (say, 100 to 500 kbits/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). True, 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 on the present rules, one only needs to look at how the field of computer networking is pretty much passing Amateur Radio by.

From ARRL "Gateway"

EOF

A Blow-By-Blow Account of the 1991 TAPR Annual Meeting

(Part 2)

Paul Williamson, KB5MU

(Editor's notes: I haven't seen a more complete, informative, and well done set of notes of a ham or any meeting. We're including Paul's notes, with his permission, virtually complete and with the most minimal editing. This article is chock full of information, but we just didn't have enough room in the last issue for all of it. This is the second part of Paul's notes.)

Dave Toth, VE3GYQ
BBS Issues

Recent FCC citations (involving a bulletin soliciting support for a political group via a 900 telephone number) have led to a high level of paranoia among BBS sysops. Message traffic may be delayed. Many sysops are killing or at least screening bulletin traffic. The HF forwarding network doesn't handle bulletins anyway, so there is little effect there. 20 meters carries most of the load, followed by 30 meters. 15, 10, and 40 also carry some. All channels are essentially saturated. Retiring BBS stations are not being replaced, in hopes of limiting contention. VHF paths are being substituted where possible, for example between VE3GYQ and W3IWI. 8 to 10 BBS stations per channel might be a reasonable target.

Meanwhile, BBS software developers are working on adding compression of forwarded message data. Some standardization is needed. W0RLI is proposing LHARC, sent in binary form through the G8BPQ software interface.

Question: Is forwarding run on a schedule, with beams pointed at the target station? Answer: Not really. The antenna is usually left fixed at a compromise heading. This is workable since each station only tries to forward to a few specific destinations. Forwarding times are theoretically slotted, but typically BBSs overrun their forwarding slots.

Question (self-asked): Have things changed in the last year? Answer: More system are running multiple connections via the G8BPQ software.

Question: Some people seem to agree with the FCC that the content of bulletins is out of control. What do sysops think? Answer: I hold ALLBBS and AMSAT message for manual review. I'm not impressed by the intelligence level exhibited by message posters OR by sysops, and I sympathize with complaints about the noise level on ALLBBS. But I think the issue should be handled within the BBS community. Local sysops should take some control. It's worth noting that the originator of the 900-number message was a repeat offender.

Dewayne Hendricks, WA8DZP
Packet in Northern California

The Northern California Packet Association (NCPA) will host the next Computer Networking Conference, September 27-28, 1991, somewhere in Silicon Valley. There were complaints about the format at the last Conference in London, so format changes (undetermined) are planned.

NCPA was formed 3 years ago to control frequency wars. It is an umbrella organization over northern CA packet groups. It is tasked with frequency coordination, and is recognized as packet frequency coordinator by NARC, the repeater coordinator for that area.

There are currently no high-speed (>1200 bps) links in regular use in northern CA. This has been tolerable because of the organization imposed on the network by NCPA. Frequencies are allocated for higher speed, but everything is operating at 1200 bps.

Nationally, NCPA serves as an educational and information distribution service. It publishes a very nice quarterly newsletter. Expect to see more publications from NCPA. The newsletter is available for $10/year.

Question: What exactly do you mean by "coordination?" Answer: Exactly the same thing meant by "coordination" of repeaters. So far we've had no disputes that weren't resolved.

Paul Newland, AD7I
METCON project

Packet is an ideal way to transmit low-tech telemetry data. He has developed a simple telemetry monitor program for an 8051 microcontroller.

A block diagram shows the 8751 microcontroller (with lots of goodies all integrated onto the microcontroller chip), up to 6 relay outputs, and current loop inputs for switch closures or outboard voltage-to-frequency (VTF) converters for measuring analog voltages. A multiplexer selects from several VTF inputs. The VTF approach was chosen because it is less susceptible to noise, and can be opto-isolated if necessary. A serial EEPROM is provided to store default values or passwords. There's support for a conventional 8-channel A/D converter. An RS-232 port connects the board to a TNC for remote control and sensing. The TNC can automatically collect periodic sensor readings, and can transmit a message when a reading changes. There's a line oriented command structure by which the remote user can control the board.

The device can be used for a remote weather station, or as a very elaborate repeater control system.

TAPR has adopted the METCON board as an official project. Pete Eaton is in charge of the development group. Lyle Johnson and Paul Newland on hardware. Kits just might be available by Dayton. Source code for the software is expected to be available, even though that will weaken the user authentication scheme and possibly embarrass Paul by revealing his coding style to the world. New software is welcome.

A prototype METCON board was shown around. A prototype VTF board was also shown. The VTF board can measure temperature directly with the addition of two components. The A/D board is not done yet. A power manager

board for battery-powered sites is under consideration. Another possible improvement would be to switch to a Signetics version of the 8051 with more I/O and more code space.

Question: would the Signetics part be code-compatible? Answer: Yes.

Question: What temperature range? Answer: The device will operate over the commercial temperature range, -20 to +85C. The sensor range is -50 to +70 or +80 C.

Question: Does it fit inside a TNC? Answer: No. But it does run on 12VDC, 100 to 150 ma.

The device can be used for a remote weather station, or as a very elaborate repeater control system. If everybody used it for repeater control, every repeater control link could be on the same frequency!

Videotape clips from the early years of packet radio (1982 to 1984)

Chuck Green, N0ADI, is shown giving a talk describing an early version of the packet protocol. It featured single-byte station addresses with a couple of bits reserved, for a maximum of 64 stations in an area. There was going to be a network control station that dynamically allocated addresses to stations entering the network. The control station would periodically broadcast the mapping from network address to station callsign. CW ID was required in those days, and there was a scheme to reduce the network overhead by having every station transmit their CW IDs simultaneously.

Another video clip showed Lyle Johnson, WA7GXD, describing the rationale for the TAPR TNC (now known as the TNC-1). Compared to the existing Vancouver VADCG TNC, it was designed to be cheaper, easier to use, and more operator-oriented. Power supply and modem were on-board, and a transmitter watchdog was provided. An alpha-test TNC was shown transmitting a packet. This was a 6502-based board running a FORTH system.

A third video clip discussed the possible applications of packet radio. Sharing an expensive computer resource (like, say, a TRS-80 Model I) was an important potential application. HF operations at 300 bps and 10 meter operation at 1200 bps were mentioned. AMTOR was proposed as a possible linking mechanism for poor HF paths. Packet operations via satellite, possibly even by portable stations, were envisioned. And an exciting blue-sky possibility was described: linking together different areas using VHF links.

One last video clip was a cautionary piece about computer viruses, that looked and sounded like something produced by the Civil Defense authorities during the '50s.

Jon Bloom, KE3Z League issues

As an aside, Jon started by mentioning that NK6K's QST article entitled "What's All This Racket About Packet?" is always held up as an example of the kind of explanatory article that QST needs.

There has been little progress on the proposed version 2.1 of the AX.25 Level 2 protocol spec. The update is still waiting for the specification in "state description language" to be completed.

At the Computer Networking Conference in Colorado Springs in 1989, the community agreed that there was a need for work on HF packet: modems, protocols, diversity reception, and spectrum management. A grant from FEMA was obtained to work on some of these issues. The terms of the grant included a provision that the government would own any intellectual property that arose from the research, and this discouraged people from working under the grant. Since then, FEMA has relented, and participants in the program will now retain all intellectual property rights. $9500 is available for HF experiments; proposals may be submitted informally to Paul Rinaldo or Jon Bloom at HQ. One possibility is to develop a new protocol for HF work, being something like a hybrid of AMTOR and AX.25. CCIR study group 8 (amateur and maritime) could be approached to make a new protocol a CCIR Recommendation.

The FCC citations against BBS sysops for relaying a message with apparent commercial content has received a lot of attention, which seems to have been what the FCC wanted. It is hoped and expected that these particular people will escape any fines. ARRL believes the FCC is taking an inconsistent position. FCC has stated officially that every station is responsible for the content of all traffic passing through it. But in the automatic control docket, FCC acknowledged that it is impossible to screen all the traffic. FCC seems to be resolving the conflict in favor of full responsibility for all stations. Perhaps they would relent if we could provide an audit trail by which the originating station alone could be held responsible.

Notice the implicit double standard, as compared to voice repeaters. Of course, if it came down to it the FCC could decide that voice repeater operators are responsible for content as well. Or, they can maintain a double standard if they wish.

Question: there are technical solutions, involving authentication schemes. Answer: the FCC just wants somebody to be responsible, and they want the amateur community to solve the problem. How we solve it is up to us, as long as we can convince the FCC that we have solved it.

Question: No matter what we do, we won't be able to stop infractions before or even while they happen. Answer: We can avoid that problem by finding a way to hold the originating station responsible.

Question: How is the audit trail in the BBS headers, apparently used by the FCC to write citations, any better evidence than the old tape recordings and DF fixes that the FCC has always refused to accept for prosecution? Question: It looks like an overzealous engineer-in-charge got carried away on this one. Answer: Maybe so, but the issue would have come up sooner or later. The head of the Private Radio Bureau intends to come out with a policy statement or rulemaking on this subject. We have some opportunity to influence this process if we act now.

Question: Does this mean that the FCC no longer considers a callsign to be meaningful? Answer: There is no ARRL position on this. KE3Z's opinion is that the callsign is useful in enforcement, but is not sufficient evidence of guilt.

Question: Is this a one-time problem? Answer: This case was just a catalyst.

Question: It's time to relicense the Microsats under some other country's authority. NK6K: It's not clear that that is possible. Even if it were, it would

Continued on page 12

TAPR Annual Meeting

Continued from page 11

make it very difficult to get the next satellite license. Also, most other countries have worse rules, not better. KE3Z: On the other hand, the US is the only country that defines 3rd party traffic to include ham-to-ham relay traffic. Comment: The UK prohibits ALL 3rd party traffic. KE3Z: It is in our best interest to prevent intruders using the network. We want some control over who uses the network for what purposes.

Question: How does this differ from some ham dialing up a 976 number on an autopatch and ...

Question: How much time will the FCC give us to resolve this issue? Answer: If we are visibly trying to implement a technical solution, we can probably have whatever time we need. If we're planning to stonewall, the deadline may be late summer or early autumn.

Question: If we come up with a solution, who will tell the FCC? Answer: Everybody. I don't know. ARRL will certainly be working on the problem. W6SWE: TAPR has set up a committee to study the problem. KE3Z: TAPR should contact Dave Sumner at HQ to coordinate efforts.

Question: Can we just ask the FCC to give us a ROM with a coded password in it? Answer: Yes, but they won't do it. They don't see this as a problem: they can just continue the current policy and cite us for violations. Notice that the FCC doesn't see any distinction between ALLBBS and any other transmission.

Question: What about the issue of the right to due process? Answer: The cited stations have that right. There is an appeal procedure. Everyone who was cited is believed to have filed an appeal. NK6K: We have to look beyond the details of this case. Their easiest defense is that the network audit trail doesn't prove they did it. That claim contradicts our claim that the network is a "pipe" and can be treated as such. This is a very dangerous regulatory position.

Question: How long ago was version 2.1 of AX.25 first discussed? Answer: Uh... about three years ago? Question: Why do we need to change the protocol? Answer: There were various issues; channel access was one. Question: Maybe we should just disband the committee. Answer: Getting protocols down on paper has always been slow work.

Question: What is the status of the HF unattended operation proposal? Answer: I'm not aware of any proposal. The STA was extended again to run through the end of this year. It'd probably be a good idea to get this whole issue resolved before the STA comes up for renewal again.

Question: There have been complaints from RTTY operators on 20 meters that packet BBS stations are encroaching on RTTY frequencies. Some claim it's a conspiracy by the STA operators. VE3GYQ: It's not STA operators, but there has been some encroachment.

Mel Whitten, K0PFX
Radios for 9600 bps Operation

Hams in Missouri are trying to build a 9600 bps network on 440 MHz. They obtained a number of Mitrek radios from a water company. They initially looked good for data, but experience shows that they are too narrow-banded for data. Widening the IF (following Mike Schroeder's article) has been a struggle, but it helped somewhat. Three links are up and running now, giving about 2400 bps throughput. These are 30-mile links; 5 to 6 mile links work a bit better.

A company called TEKK makes a very small 2-watt data transceiver that seems ideal for this application. They currently come for commercial frequencies around 461 MHz, but a ham band version is possible. With G3RUH modems, interfacing is easy and bit error rate tests give good results. They run all day without retries. Mike Chepponis, K3MC, has moved a couple of the commercial-band TEKK radios into the amateur band.

Dewayne Hendricks, WA8DZP
K3MC proxy report

One of the TEKK radios, mounted in a chassis with a Kantronics G3RUH modem, was passed around. The TEKK radio costs only $150 in single unit quantities! The radio is tiny. Recovery time less than 8ms. Sensitivity 0.3 microvolts for 12dB SINAD. Crystal controlled, single channel.

He is also working with K3MC on 900 MHz Part 15 spread spectrum devices. A tiny 121kbps 1W 900MHz data transceiver was passed around. It costs about $150. There was a session on wireless networking at the recent Hacker's Conference. They discussed the new no-code amateur license, but weren't very excited about it: the content restrictions imposed on the amateur service are too onerous. They'd rather stick with the Part 15 devices, which may be used to transmit any kind of messages.

Most of the commercial units are direct sequence spread spectrum. One recent unit is frequency hopped instead. Chips sets are becoming available for spread spectrum. More information will be presented at the next Computer Networking Conference.

K3MC has left Apple Computer.

Apple Computer filed a petition with the FCC a month ago, seeking to create a personal data communications service. The comments deadline is March 11. They don't think Part 15 devices are suitable. They want 1 watt, 1 Mbps, at 1.8 GHz. They want some different tradeoffs between power and antenna directionality. They propose a phase-in of frequencies. The IEEE has formed a committee for wireless LAN issues. WA8DZP (and soon K3MC) is a member of the committee.

Chuck Green, N0ADI
TAPR Production

Did you ever wonder about how all the parts in your TAPR kits got there? N0ADI's wife does all the kitting. His spare room (which was going to be the hamshack...) is the TAPR warehouse. In the early days of the TNC2, the warehouse took over the family room and part of the living room, as well. 2700 TNC-1 kits and 1200 TNC-2 kits were packaged, and countless smaller kits. 2500 kits, all small, were shipped last year.

Question: How many K9NG modems? Answer: A few hundred.

When a production run ends, TAPR retains a quantity of spare parts. If you need a spare part, they probably have it. Full kits of parts for boards are not available, though.

N0ADI also has possession of a computer owned by TAPR for PC board layout using ProCAD software. It was on display in the meeting room, with the very complex layout of the DSP board on the screen. The DSP board holds 67 ICs. Notice that the bottom rear corner of the

board is shaved off to permit insertion from the top of the PC chassis.

Question: How many hours did it take to lay out the DSP-1? Answer: A couple hundred.

Question: We have 8 K9NG modems unbuilt; can we get kits of parts without boards to fill them? Answer: The theory was that the parts not included in the partial kit were easy to obtain. So no, we don't plan to issue a parts-only kit.

Don Lemley, N4PCR
the PackeTen Switch

[This talk contained a lot of detail given at lightning speed. I couldn't begin to write it all down. The following is some of what I did catch - Paul]

Why the PackeTen switch? Overloaded networks. Advanced applications are not practical at the low bandwidths currently available. There were political problems. He decided to focus on the digital side of the problem, since that is where his expertise lies. He wanted to provide an off-the-shelf solution that would support the fastest modems and radios available, up to 56 kbps, and future platforms to 1 Mbps. It provides backwards compatibility to the existing users. And at lower cost than the usual configuration of many TNCs.

After the upgrade, the network had fewer nodes, was more organized, and supported higher data rates.

The PackeTen features a MC68302 special-purpose processor running at 16 or 20 MHz. 3 high-speed synchronous or asynchronous channels, with an aggregate throughput of 2 Mbps. Clocking is software configurable. EEPROM memory stores configuration info. CMOS is used for low power. 2 megabytes each of RAM and ROM can be installed.

The card comes in two versions: standalone and PC plugin. The PC plugin card has a very fast dualport memory interface to the PC. It can use an 8 or 16-bit interface to the PC bus.

The PackeTen runs a customized version of the KA9Q NOS networking software ("NOS-in-a-box"). This version supports NET/ROM for backwards compatibility with NET/ROM networks and users. And of course, TCP/IP users can use its more sophisticated features.

Pictures of the Chicago area network before and after upgrades using the PackeTen were shown. After the upgrade, the network had fewer nodes, was more organized, and supported higher data rates.

Question: What's the name and address of the company? Answer: Catch me after the meeting.

Question: If the Chicago group was like most, the original network resources were owned by a variety of clubs and individuals. How did you deal with this when upgrading the network? Answer: The IP users group put together the funds to build the new network. When it was up and working better than the old network, the other stuff just faded away and the users switched to the new network.

Question: Does the Chicago network use the PC plugin card or the standalone version? Answer: Both. The PC version is used in the nameserver, and the standalone version is used in the switches.

Question: Does the diskless node require a custom BIOS, or what? Answer: NOSINABOX takes care of all that.

Question: What frequency is all this networking done on? Answer: 70 cm.

Question: What's the price? Answer: $700 for the standalone version, $800 for the PC version.

Question: What's this 4800 bps landline link shown in your diagram? Answer: That's really a 1.2 GHz link to a tower that hosts the wormhole to California.

Bdale Garbee, N3EUA
Colorado report

Welcome to ex-members of the former Rocky Mountain Packet Radio Association. As RMPRA disbanded, a group of new faces formed COPA, the Colorado Packet Association. Bdale ended up chairman of the Technical Standards Committee of COPA.

The network just didn't work. Now they are focussing on east-west linking across the mountains, instead of the former emphasis on north-south linking along the front range. A new backbone is planned for this summer. The current network works so poorly that backwards compatibility isn't much of an issue.

Lack of organization has been a problem. Not everyone understands the distinction between an occasional path and a reliable path. Many of the paths currently in use rely on knife-edge propagation, which is not suitable for high-speed data links. Site selection and service goals were the main issues. It was necessary to use point-to-point line-of-sight links of less than 50 miles. 300-mile links between 14000 foot peaks were the wrong answer.

The plan is to put 10GHz links at 6 nodes, arranged in a linear backbone. With two backbone links and two user access ports at each node, they needed 4-port controllers. Given that, the cost differential between the usual low-performance multi-TNC implementation and the PackeTen was small. They bought 3 PackeTen standalone units, with 3 more to be obtained soon. A working group is trying to make the 10 GHz 1 Mbps modems designed by N6GN and others mountain-worthy.

They want to make use of full duplex to conquer the hidden terminal problem that tall mountains produce. They have permission for a duplex machine on Pikes Peak. A crossband duplex machine is already in operation near N3EUA.

It is hoped that by the time of the Computer Networking Conference, bare PCBs or perhaps even kits will be available. They are still investigating interface issues for 10 GHz modems. The current theory is to add the circuitry to the modem, so they can be connected directly to the PackeTen. There is some thought of varying the data rate as conditions change.

Phil Anderson, W0XI
Kantronics

Last year, the market was depressed, but since September volume has been up surprisingly. Commercial customers are buying TNCs for HF and VHF, and even some 2400 bps QPSK units. Amoco and Tennessee Gas are using TNCs for sending data to operators in mobile units.

The latest product from Kantronics is the TelemetryUnit. A front panel was passed around. The TU hooks up between instruments and a TNC to relay telemetry. It features screw terminals on the back panel to ease field installation. Firmware is available that supports an

Continued on page 14

TAPR Annual Meeting

Continued from page 13

anemometer, wind direction sensor, ratiometric A/D converter, temperature sensor, and rain gauge. They're still looking for a suitable pressure sensor. This firmware gives a text-based human interface on the data port. The operator specifies the sample rate, and it automatically collects the data. You then ask it for a report, and it dumps the data to you. Sampling everything every 5 minutes, there's room for a few days info. Sampling just temperature every 30 minutes, it'll go a year before it fills up. Another firmware version is available that provides a general units-translation feature, with user-specified units.

Kantronics is developing the D4-10 data transceiver. They will be seeking FCC Part 15 approval soon. It has microphone, analog data, and digital data interfaces. Two channels, crystal controlled. They have some tricks to make TX/RX switching fast. The receiver filtration scheme and major parts choices were discussed. The built-in slicer can tolerate up to 4 kHz of frequency error. Spectrum analyzer displays for various tests were shown.

They hope to have the D4-10 available by Dayton. Pricing is not yet determined, but it will probably be around $300.

Question: Do commercial band users have trouble getting licensed to use data transmission on shared voice channels? Answer: We've found that most 2-way radio shops don't understand data. They estimate that 50 shops in the country can really handle it. On a shared voice repeater, data is secondary to voice. There is some movement toward data in trunked SMR. Nobody seems to know where the data market is. There's more data on HF, in ship-to-shore, governmental, and utility applications.

Question: What about public safety services? Answer: Riverside County, CA is very enthusiastic about data communications. But each user needs custom software, and that's not practical. For example, Amoco cut its 30-man communications staff to 2 after the oil embargo. In that kind of situation, companies need turnkey solutions.

Question: Have you tested against radar QRM? Answer: No. The radio was tested in Chicago. Pagers have been something of a problem. In an earlier model, aircraft frequencies fell on an IF image and caused problems.

Gwyn Ready, W1BEL PacComm

PacComm's EM-NB96 9600 bps data communications line is growing. The modem has a new feature: the modem disconnect is brought out so that other modems can be chained onto the same TNC. The NB96 modem can be connected directly to the TEKK radio; PacComm worked with TEKK as a beta tester for data applications. They work very well on good RF paths. In commercial service, they specify the modems to work with a path of a certain quieting, and the user can't complain if they don't work on crummy links.

The TEKK radio will be available on amateur frequencies. They'll be tunable from 420 to 440 MHz, crystal controlled. Some should be available at Dayton. They're looking for input as to what frequencies should be made available.

The TINY-2 PLUS is an add-in board for the TINY-2 TNC. It's aimed at experimenters, with other features intended to encourage volume sales. It has open squelch DCD, a hardware clock, room for 512K of extra RAM, and 3 extra EPROM sockets. The ROMs can be selected by software. You can put RAM in the EPROM sockets and download code to it. The serial ports have LEDs for debugging. A mini-BBS and remote commanding are supported by the standard firmware. A monitor EPROM is available. The add-in board draws about 40 ma.

There's also a smaller, cheaper add-in board that just expands the memory. It plugs into the Z80 socket, and gives 128K of RAM expansion.

One of the first PacComm Handi-Packet TNCs was recently delivered to the Soviet space station Mir. There seems to be a bit of a problem with user training; the cosmonauts don't understand all of the features.

TAPR Annual Business Meeting

President Bob Nielsen, W6SWE, called the TAPR Annual Meeting to order at 4:23 PM. He introduced the new board members and officers. Bob Hansen, N2GDE, is the new editor of PSR.

Greg Jones, WD5IVD, is now the manager of the packetRadio project. Boards have been prototyped and debugged, but still need some work. No date is promised. A more complete report is expected later this year.

The METCON and DSP projects were discussed in the board meeting.

A Guide to Operating Packet is to be published in time for sales at Dayton.

The packet video featuring Pete Eaton, WB9FLW, is to be updated this year.

A Committee to develop a TAPR position on the current regulatory issues was appointed: NK6K, N3EUA, VE3GYQ.

METCON is the only new project that was officially adopted, but some other ideas are cooking in the back room. New ideas and project proposals are solicited; you don't need to be a member of the inner circle (or even a member of TAPR) to propose a project.

Prices for software and kits will probably be increased before Dayton.

Greg Jones, WD5IVD, gave the financial report. Total assets are around $103,000. Revenue this year was about $79,000, mostly from the sales of small kits. OEM licensing revenues from TNC-2 sales have all expired. The membership has increased from 700 to 1200 members. This year's net is $2000. Quite a bit was spent on R&D.

Question: What liabilities are there? Answer: The liabilities sheet was shown. One liability is a member services reserve. This reserve covers the cost of quarterly PSRs for the duration of all paid-up memberships, so that the Board can't spend the money that's already promised to members.

In August, the bookkeeping switched to a new, more automated service in Austin, TX. The new arrangement gives more services for the same price.

Question: Do dues cover costs? Answer: About 80% of dues pays for PSR. The rest depends on what assumptions you make about how Heather's time is spent.

NK6K: Notice that there are no engineering salaries in the budget. We only pay for services that engineers won't do.

Question: Why are Board meetings closed? Maybe a Member-At-Large would be a good idea. Answer (NK6K): Some issues are too volatile to discuss in a large group. Some Board members think the Board is too large anyway.

Board meetings aren't usually officially closed, but sometimes they have to be. N3EUA: Note that the Board does meet continuously via Compu$erve. You can bring issues or proposals before the Board at any time of year.

Question (joking): Where is the Version 4.0 of the TNC-1 software? Answer (NK6K): Nowhere.

Steve Hall, WM6P
HF Diversity Reception

Experiments with diversity reception for HF packet have been carried out. The scheme used two separate antennas, receivers, and modems. Software provided by Kantronics was used to keep statistics on packets copied by both TNCs and packets copied by one but not the other. The receivers were mostly listening to the 20 meter BBS forwarding channel. This provided a variety of locations, signal strengths, and angles of arrival.

The results were surprisingly consistent: A second receiver gave about 50% improvement in packets received. For instance, if the A channel receives 4000 packets correctly, typically the B channel would receive an additional 2000 packets that A didn't copy. This performance level was largely independent of the quality of equipment used on the B channel. Even relatively inferior equipment (R390 and R388 surplus receivers with random wire antennas) provided about 50% additional packets, even when relatively first-class equipment (TS940S receiver on a monoband beam) was used on the first channel.

The results were also largely independent of the antenna configuration used. The only pair of antennas that didn't exhibit good diversity was a pair of horizontal dipoles at right angles with co-located feedpoints. Parallel dipoles spaced a half wave apart gave good results. Comparative tests were difficult, since ionospheric conditions changed performance more radically that antenna selection.

In light fading, diversity improvement fell to about 20% additional packets. When fading was heavy, diversity improvement was larger, since the two channels tend to fade independently.

Another test configuration using a dual-port DRSI PC*PA board with software provided by Andy DiMartini gave similar results.

So far, the diversity combining tests have been a laboratory curiosity. The next step is to make a combiner box that will allow two TNCs to handshake and do diversity receiving automagically. He has talked to manufacturers, with lukewarm results. Jon Bloom, KE3Z, is interested, and they plan to move ahead with a prototype that will interconnect two KISS TNCs.

Question: What spatial separation was required to get space diversity? Answer: A half wave gave nearly full diversity.

Question: When you watched the S meters on the two receivers, did you observe fading that was too fast for packet-level combining to cover? Answer: Yes, there was some fast fading. It was hard to sort out the effects of collisions from those of fading. We tried some tests with a lower baud rate (100 bps), which seemed to indicate that the long packet durations overwhelmed any advantage.

Question: Did you try diversity combining using analog voting? Answer: No. That scheme would assume that the stronger packet is the good one. Observations show that sometimes it's the weaker one that (a) can be demodulated successfully and (b) is the packet you want.

A second receiver [consistantly] gave about 50% improvement in packets received.

Question: Did you try polarization diversity? Answer: Yes. But with the ionosphere changing faster than the antenna configurations, it was hard to draw any conclusions.

Question: In the old RTTY days, we sometimes ran two receivers with a common AGC so that the strong signal would overwhelm a weaker one. Answer: Again, that would assume that strong equals good. I didn't do it that way.

Question: What packet length was used? Answer: All lengths. Whatever was on the channel.

Question: This would work better with shorter packets, wouldn't it? Answer: It seemed to work OK with random lengths.

Question: Did you ever see better than 50% improvement? Answer: Yes, we saw 60% sometimes. But there were also times when there was little fading, and both receivers were copying nearly every packet.

Question: How many packets were missed? Answer: Many packets were lost to collisions. Sometimes one channel would see a collision, but the other channel would copy one of the packets.

Tests were run near the MUF and well below it. It didn't seem to matter.

Question: Will the results be published? Answer: Yes, in some ARRL publication or other.

Question: A local company, Dovetron, has done diversity work. Your results correlate with their claims. This technique has been around a long time for RTTY. Answer: Yes, I did play with RTTY some. It worked there as well. Also on AMTOR. Not discarding entire packets gave better improvements, but it required human intelligence to determine which receiver had the right data. With packet, that process is automated by the CRC.

Question: Could you explain how a strong signal could be worse than a weak signal? Answer: There are only two kinds of packets: perfect and useless. Any packet you can demodulate is good. Comment: Assume a flat earth, and fixed ionosphere height, and raytrace a few angles. You'll quickly see the interference pattern, resulting in areas with no signal, and areas with strong signal.

Question: Can you propose a model for a strong, bad signal? Answer: Sure. Two signals colliding makes a big signal. Comment: Bit smearing by multipath can ruin a packet, too. Answer: Another case is when the weaker signal is the one you want.

Tests were also performed on military signals that were strong and had a clear channel. Signals were still observed that could not be copied even though they were loud.

Question: How did you perform the low baud rate tests? Answer: With a cooperating connected station.

Question: At low baud rates, did you use a correspondingly narrow filter? Answer: No, we used the same 500Hz filters for all speeds.

Question: Did you see frames with no detectable fading that you still didn't

Continued on page 16

TAPR Annual Meeting

Continued from page 15

copy? Answer: Yes, and I can't really explain them.

Phil Karn, KA9Q
NET/NOS status

Anders Klemets, SM0RGV, has evolved the simple mailbox in NOS into a fullscale BBS.

The RSPF (Radio Shortest-Path-First) protocol has been added to NOS. It's more stable than algorithms like the one NET/ROM uses when paths go up and down. Each node only keeps track of the routes to his neighbors. The information is distributed by flooding, and each node is able to compute a map of the network. RSPF mirrors OSPF, an Internet protocol.

PPP, the Point-to-Point Protocol, has been implemented by Katy Stevens. This serves as a replacement for SLIP (like KISS) on wired links. She has also implemented TCP header compression, which replaces the usual 40 bytes of header overhead with 3 bytes. This is especially interesting when sending a lot of single-character packets, as when doing remote keyboard echoing. Anders has ported the compression to the AX.25 module, but it's not as exciting there because of the AX.25 header and keyup delay overhead.

Anders has implemented stream compression based on the LZW algorithm. This scheme is transparent to applications. It works reasonably well for large file transfers, but isn't very useful for small files like mail messages.

NOTE: A lot of work on NET/NOS has been done by others, but KA9Q gets lots of gripes and questions about parts of the software he didn't write and may never even have seen. Please don't call him unless you're sure it's his part of the code that's a problem.

He's been trying to get the code running with some faster modems. He's been running a 56kbps WA4DSY modem on 220 MHz for a long time, but the host interface is a problem. His HS driver uses a PC plug-in card with a 8530 chip without DMA support. Since the machine can't service an interrupt per character, the HS driver has to sit in a spin loop while receiving a packet. This causes the machine to freeze up. In the last few months, two new cards have appeared that support DMA: the Ottawa Packet Interface (PI) board, and the DMASYNC card by WA6FXT and N6XJJ. The DMASYNC uses a WD1950 instead of an 8530, so it has only one channel. Since there's only one DMA channel available in a PC anyway, that's no big loss.

Question: Doesn't anybody make a card with a shared-memory interface? Answer: The PackeTen is the only one, and it's pretty expensive. Both of these DMA-supporting cards are cheap. You don't need a fast machine to run NET as a gateway or switch.

Last year KA9Q described a collision avoidance algorithm, and he's still working on that. He now has an idea to modify P-persistence dynamically. The TNC would be slow to take the channel after hearing a packet that needs to be acknowledged by someone else, and fast to take the channel to acknowledge a packet for itself. This might help mitigate the hidden terminal problem. It might also be useful to enhance the MHEARD feature to keep track of hidden terminals, so as to try to avoid transmitting when a hidden terminal is probably transmitting.

This kind of enhancement can even help on a point to point link, by reducing the collisions between data frames and acknowledgement frames. With the HS driver, back-to-back data frames had a short gap between them, just long enough for the other station to jump in and collide with the next data frame.

Question: What about your work with authentication schemes? Answer: I'm working on several schemes. Some are weak against an active attacker, and some aren't.

Question: If we have a good system of authentication, there may be problems with export restrictions. Answer: My understanding is that authentication systems (unlike crypto systems) are not a problem. Control of export of authentication systems has been transferred from the State Department to the Commerce Department.

KA9Q has implemented a scheme for transmitting passwords over the air. The method is misnamed MINK, for Master InterNet Key. It's based on the idea of a one-way function: a mathematical function that is relatively easy to compute, but whose inverse function is very difficult to compute. The standard crypto system DES is an example of a one-way function.

Aside: Shamir (the S in "RSA") has found an attack that breaks many simple variations of DES. Under this attack, DES is exactly as difficult to analyze as under the brute force approach. If this attack is the best possible, this shows that the choice of key-size (56 bits) was exactly right. If so, charges that the NSA reduced DES's key-size in order to weaken its security are ill-founded.

MINK uses a one-way function called MD4. MD4 produces a 128-bit output from any size input. The scheme is to take your (secret) key, and apply MD4 to it many times, say n times. Call this result $F_n(x)$, where x is your password. Since the inverse of MD4 is hard to compute, it will be hard to compute $F_{n-1}(x)$ given only $F_n(x)$. So it's safe to transmit $F_n(x)$ over the air, provided that in the next session you use $F_{n-1}(x)$, and $F_{n-2}(x)$ in the one after that, and so on. Since MD4 itself is easy to compute, the server you're logging into can easily verify that the password you're using now, $F_{n-1}(x)$, corresponds correctly to the one you used last time, $F_n(x)$, by simply computing $F_1(F_{n-1}(x))$.

This scheme is secure (to the extent MD4 is really hard to compute) against passive eavesdroppers, who only try to learn your password by listening to what you transmit. It is not at all secure against an active attacker, who may transmit messages of his own in an attempt to gain access to your account. Also note that the computer itself doesn't have your current password; it only has your previous password.

MD4 is used instead of DES, which is probably much more secure, because DES is too hard to compute in the forward direction. Since MINK involves computing many iterations of the crypto algorithm every time a new password is needed, a difficult-to-compute function is impractical.

Question: Doesn't this assume that the users have local computers that can compute the encrypted passwords? Answer: Yes, that is a potential problem. Perhaps the users could be asked to have smart cards to compute passwords. For the user who does have a computer, he needn't worry about MINK at all. The telnet program he uses to log into the remote computer can easily respond to the MINK password prompt automatically.

Question: If you have a password with many bits, don't you have a problem with

Crazy Characters

Larry Kenney, WB9LOZ
NCPA Education Coordinator

(Editor's note: Ever wonder about some of those weird things you've seen on your terminal's screen? Well, read on... Just remember that what you see on your terminal might not look the same as is described by Larry.)

Have you noticed the occasional [A [B [C [D arrows and other "weird" characters in the messages you've read? Maybe you've had a problem yourself where they've ended up in messages you've entered. The keys on your keyboard can occasionally give you something you didn't ask for.

When using some of the word processing programs to compose your messages and when using some of the popular communications programs, you can correct errors by using the left and right arrow keys, the ones on the 4 and 6 keys of the keypad, in combination with the DEL key. The results you see on the screen are not always what you'll get when the message is sent to the BBS, however.

The left arrow key converts to [D and the right arrow key gives you a [C in the text. An up-arrow turns into [A, the down-arrow becomes [B, HOME turns into [H and the END key shows as [K.

To avoid these characters, make your corrections by using only the BACKSPACE key. BACKSPACE to the error and then retype the line. Don't use the left arrow key to get to the error nor the right arrow key to return to your original spot in the text or you could be adding lots of [D[D[D[D[D[C[C[C[C[C to your message.

73, Larry,
WB9LOZ @ W6PW

EOF

TAPR Annual Meeting

Continued from page 11

users mistyping a long numerical password? Answer: A standard way around this problem is to use mnemonic words. You assign a list of, say, 2048 standard common words. Each word can then be assigned a unique 6-bit number. So if your password is 66 bits long, you just have to remember (and type in) a sequence of 11 common words.

Question: Doesn't this system demand that you always log in from the same place? Answer: No. The server computer maintains all the state information. When you try to log in, it tells you what *n* it expects you to use. For example, a login dialog might look like this:

```
login: karn
MINK 99 KA9Q1
Password:_
```

So you have *n*, and the input to the function. You just run MD4 with your secret key *n* times on the seed "KA9Q1" and type the result back to the computer. If you're on a secure link instead of a radio link, you can also type your regular (plaintext) password.

Also notice that if you don't trust the computer you're using to log in from, you can't let it do the password computation for you. That would involve telling it your secret password. The only secure alternative is to carry your own password computer with you. We use Atari Portfolios.

Question: Is MD4 available? Answer: I will be releasing a package soon.

Question: What are the relative advantages and disadvantages of Unix vs. DOS for a TCP/IP server? Answer: The most important thing is to get a recent version of TCP/IP with the Van Jacobson enhancements. I recommend that the best way to put a Unix box on the air is to use a dumb PC as an ethernet to radio TCP/IP gateway. The gateway PC can handle your dialup link to work, too.

Question: Can't I just connect a TNC to a TTY port? Answer: Yes, you can, but that only handles one interactive user. With a TCP/IP port you can support more users and get more functionality. With BSD Unix for the '386 coming out, the art of hacking TCP/IP support into Unix will become obsolete. Besides, putting NOS into Unix or even putting all sorts of features into NOS is counter to the original spirit of NOS: to introduce TCP/IP to amateur radio, for cheap.

Question: What flavors does NET/NOS come in, and where can we get them? Answer: If you have Internet access, ftp to thumper.bellcore.com ([128.96.41.1]) and log in with username anonymous and password your name. Look in /pub/ka9q; there are different subdirectories for different versions. If you wish to contribute something, put it in /pub/ka9q/incoming. I can't handle any other distribution mechanism. The code is also available on several dialup BBS systems.

Question: What about the TAPR library? N3EUA: I have given up on packaging the KA9Q code for releases. It was just too time-consuming. We've been at this project for 5 years!

Question: What are the difficulties of configuration control? What works and what doesn't for a widely-distributed group effort like NOS? Answer: Everything works fine if people are working in separate areas. For instance, Anders work on the mailbox code was easily integrated back into the standard release. If two people are working on the same module, there's a problem. In a volunteer project, you can't use someone's promise to do a task as a locking mechanism. For example, two different people fixed the domain name system simultaneously, and now I have to choose one and snub the other. N3EUA: the 890421 release of NET was a big integration problem, with many different sets of conflicting changes. One developer made wholesale changes (some of which were unnecessary), and that code is still a separate branch that will probably never be integrated.

Ron Bates, AG7H radio telescopes

Ron Bates, AG7H, works at NRAO with the radio telescopes on Kitt Peak. He invited interested parties to go on a tour of the telescopes after the meeting. Provided the road isn't blocked by a rock slide!

Lyle Johnson, WA7GXD, thanked everyone for coming to the meeting.

See you next year!

EOF

NCPA Board Meeting Minutes

June 2, 1991
General Parametrics Corp., Richmond

Meeting was not formally called to order (only 3 board members present, 4 required for quorum). The following board members were present, Eric WD6CMU, Steve KA6ETB, and Dennis KA6FUB. Others at meeting Bruce, ????? (DX group), Bob NOARY, Ron N6QIY, Gary N6PAW, Fred K6RAU and Roy, AA4RE.

After introductions we discussed if we could proceed with meeting or not. Fred looked over By Laws and it was confirmed that without 4 board members we could not vote on any issues. It was decided however to continue with a informal meeting to address any issues that could be handled without requiring a board decision.

Eric discussed the problem with members of the board that were not holding to commitments, ie attending meetings and following though on promises made. We tried to contact Pat N6QMY to see if we could get him to give us a phone proxy to vote on issues. No contact was made.

Packet Band Plans Roy passed out revised band plans as of 2 Jun 91. Changes are as follows:

220 MHz - 223.56 was change from node uplink to keyboard 223.70 from keyboard to node uplink (Monterey Bay) and TCP/IP (Sac Valley) The problem with the EBAY Lan moving to 223.66 was brought up. The freq is also used as the SOCAL link and there is a conflict with the band plan there. After discussing the issues it was decided that Roy would contact NARC and see if we can continue to us 223.54 for EBAY and the SOCAL link. The second option would be to reassign 223.56 as the EBAY and SOCAL freq and reassign 223.66 as keyboard if we can get concurrence with the SOCAL group to get them to move to .56. The final option would be to try to find a location to install new node that would allow use of 223.66 for EBAY and either 223.54 or 223.56 for SOCAL link. Roy would proceed with the options in order listed and get back to board. 440 MHz 433.25 changed from DX (100 KHz wide) to Experimental 433.39 to DX packet cluster 433.41 to BBS Interlink 433.45 to BBS Interlink

900 MHz 904.000 2 MHz wide 916.000 2 MHz wide 916.990 BBS link (non-interfere with 916.000 There was some discussion that mode channels may be needed so Roy is going to split up the 904 channel into 20 and 100 KHz channels and will sent the board the new plan.

Dennis had a bulletin that was being sent @ SACVLY about the need for a RACES only channel. Roy had talked to them before and if he was asked again the policy still stands that no channels can be assigned to use only in emergencies.

Roy said that he was contacted about the need for a Hospital Net. He had asked for some additional info because it seemed this was for Kaiser only he got no reply. We figured this has become a dead item.

Grandfathering The issue of grandfathering was talked about. We had received some requests that the subject of WA6RHD's BBS on 145.01 be discussed. The keyboard users all would like RDH to move to A BBS channel. The items of interest where why Dennis continues to operate on .01, are there any technical or operational reasons, if he stays on .01 is there anything that he could do to his system that the keyboard users would accept. It was decided that we need to contact Dennis and find out his side of the issue to see if something can be worked out. Dennis, KA6FUB, said that he would contact RDH and see if something can be worked out and would get back to the board with any recommendations. Also because there was only 3 board members present no decision could have been made today.

Membership, Dues, Funds. Because the secretary and treasure where not present we could not determine total membership or account balances. Membership is down however and we discussed ways of increasing numbers. The Foothill Flea Market has in the past been a good source for recruiting but we have not had anyone there for awhile. Dennis KA6FUB said that he was going to the next one on 8 June and that he would get a table and handle it. Bob, NOARY, said that he would also help so each could look around at the other tables. We are going to have to decide on how many news letters we are going to have printed in the future. In the past 500 have been printed but with membership only at about 100 now we many have to reduce this to keep from breaking the bank. We need to check with Glen at HRO to find out if payment is going to be made for sales at there stores. Steve, KA6ETB, had info on membership cards. Prices for cards ranged from $23.90 for single color non-numbered cards in lots of 100 to $87.00 for two color numbered cards in lots of 500. The idea of getting the cards in post card format was discussed and all thought in was a good idea. Steve will contact the printer again and get the cost.

FCC Citations of BBS Operators Eric,WD6CMU, brought up the subject of the citations issued by the FCC to the BBS operators involved in the 900 number message. The FCC is proposing that both originating stations and the BBS that station uses to enter a message into the system can be held responsible for the message content. At the present time it appears that the ARRL is going along with this proposal. The consciences of the board members present however is that only the originating station should be held responsible as is the case with voice repeaters. It was decided that the secretary will send a letter to the ARRL and FCC with NCPA's view on this matter.

Finally Gray, N6PAW, showed off a 56K Baud radio he had. It was all put together and ready to go on 433 MHz however he had not done any testing because the second unit a friend was working on was delayed. The concept looked good but we did have questions on how it would interface with the existing BBS forwarding network.

The meeting broke up at about 12:30

September 8, 1991
Alameda County Emergency Training Center, San Leandro

Board Members present: Eric WD6CMU Larry WB9LOZ Steve KA6ETB Patrick N6QMY (Mike K3MC arrived late); two guests also attended

Eric:Opened meeting at 09:25

Election of officers: Pres: Eric WD6CMU; Vpres: Larry WB9LOZ; Tres: Patrick N6QMY; Sec: Dewayne WA8DZP; Editor: Steve KA6ETB.

Membership: Problems with yearly membership. People don't like getting one year lump sum. Tres. does not like yearly fee for news letter. By a vote of 4-0, the board directs the secretary to take the necessary steps to convert to a conventional term of membership.

Status check on membership cards: Steve (KA6ETB) slipped. Will be businness cards - 500 count.

BBS channel on 443.37?Now marked as expermintal. Interested parties did not attend. The issue was tables, Eric will refer back for more info.

Grandfathered BBS use on KBD-KBD channel. Board recommends RDH and KBD group try to work out differences at CNC. However, if RDH wants to remain, he is grandfathered, and if nothing can be worked out, he can stay. Eric will work as medeator between the groups.

BBS software standards: Unanimous opinion that continental designators, software standards, etc. are not within NCPA's purview

Should NCPA publish TCP/IP handbook? Larry and Steve will take this up.

Should NCPA go national? We will try advertising "Intro to Packet" in QST classifieds. The board authorized expenditures for at lease one month's ad, possibly more—to be evaluated later.

Treasurer's report: Current balance: $1106.45. Pat will contact KA6FUB for proceeds from flea market sales and AA6ER (Glen) for newsletter sales from HRO. Pat will follow up with Dewayne on better handling of PO box mail.

Eric: What does the NCPA board members have to do at the CNC? Unknown if anything at this time. Next CNC meeting will be Sept 22.

BBS forwarding/220 move/9600 baud backbone. Refer to NCXPN. Eric gave an overview for general info. K3MC doing research with Tekk radios, but running into problems. KA6FUB using Motorla radios , tests should start Real Soon Now.

Steve resigns as NCPA Emergency coordiantor due to almost complete lack of cooperation from established emergency communication service organizations.

Meeting adjourned at 11:34 EOF

Meet The New NCPA Board

Mike Chepponis, K3MC

I'm an avid packeteer. I've been running a BBS since 1985, back on my Big Board (820 was descended from the Big Board). I've run that BBS from my various QTHs of Pittsburgh, PA, Boston/Cambridge, MA and now Fremont. I quickly became a TCP/IP convert, and used to run KA9Q's code on the Big Board when his stuff worked under CP/M. With Phil Karn (KA9Q), wrote KISS TNC spec; wrote TNC-2 version of KISS. Built Awesome I/O card (but for various reasons, it is not yet available). Eager to have all digital services work together to have the best possible future for Ham Radio: DXPSN, BBS, TCP/IP, Keyboarders, Emergency Handlers, Traffic Handlers, etc. With the strong start of our nationally-respected NCPA, we can make a difference here in Northern California (still the best place on the planet for packet radio.).

Steve Harding, KA6ETB

This is my second term as a member of the Board of Directors. I have held a Tech class license since 1979. Since that time, my primary interest has been formal traffic handling. I have been a NCS for the NCN-VHF session on and off for several years. Since discovering packet, I have been amazed at how well the system works in delivering traffic and, as NCN NTS packet manager, I have been actively working to improve the NTS packet system.

My wife, Bev, holds amateur license KA6TCT.

Larry Kenney, WB9LOZ

I received my first ham license, the Novice, and the call KN1TGZ, in 1961 while in high school in New Hampshire. I received his present call in 1973 while living in Chicago, Illinois. I am a General Class ham. I got involved in packet radio in 1985 and established the W6PW-3 BBS in San Francisco in November, 1986. I am the Education Coordinator of the NCPA and wrote the *Introduction to Packet Radio*, available as a booklet from the NCPA and as files on many BBSs. The series of articles was originally written as a monthly column for the San Francisco Amateur Radio Club, of which I have been a member since moving to San Francisco in 1979. I have presented several talks on the basics of packet radio at seminars and at club meetings and send out informative bulletins on a regular basis covering various aspects of packet for users in Northern California.

Dennis Matzen, KA6FUB

I live in Martinez and work in the Support Services Division of Contra Costa Co Sheriff Department. My title is Communications Systems Manager and my duties include managing the department's Radios, Comm Center equipment, Telephone equipment and Data systems. My ham radio interest include Packet Radio (BBS SYSOP and Node operator) and repeater operation on VHF & UHF. I am the sysop of the KA6FUB BBS located at the Contra Costa Co EOC and have helped with the installation and maint of many packet nodes both in Contra Costa Co and the link to Oregon. My interest with repeaters keeps me busy also helping maintain the CCRA repeater systems in Contra Costa County.

Patrick Mulrooney, N6QMY

I became involved with Packet with the BBS at the National Weather Service station in Redwood City. I became a BBS sysop when I moved to Fremont and did not have a good connection to a full service BBS. I spend most of my FM voice time on KU6V/R (now on 223.72 moving to ?) My wife Theresa is also a tech — KB6UCZ.

I work for Ungermann-Bass in Santa Clara supporting our international LAN and WAN and I act as site Postmaster for the Internet. I am activly working on converting our corporate LAN from XNS to TCP/IP.

Eric Williams, WD6CMU

Shortly after arriving in Berkeley for college in 1977, I earned my first ham license. In 1985, N6FQR, NI6A and I put W6CUS-1 on the air, at the time the only Xerox 820-based BBS with a hard disk (that we knew of). Don and I also founded the northern California sysop association which, in 1987, became the present-day NCPA, and I was elected its first president. Somewhere around that time, I finished writing a multi-user BBS program which runs under OS9/68000, a multi-tasking multi-user operating system, and the WD6CMU BBS went on the air. Shortly thereafter, I implimented the first White Pages server.

I work as a programmer for General Parametrics Corp. in Berkeley, which produces color business graphics products.

NCPA Directors

Eric Williams, WD6CMU
WD6CMU @ WD6CMU
415-237-9909

Steve Harding, KA6ETB
KA6ETB @ N6LDL
408-996-2689

Patrick Mulrooney, N6QMY
N6QMY @ N6QMY
408-562-5659

Dewayne Hendricks, WA8DZP
WA8DZP @ K3MC

Larry Kenney, WB9LOZ
WB9LOZ @ W6PW
415-821-2666

Dennis Matzen, KA6FUB
KA6FUB @ KA6FUB

NCPA Officers

President:
Eric Williams, WD6CMU
WD6CMU @ WD6CMU

Vice-President:
Larry Kenney, WB9LOZ
WB9LOZ @ W6PW

Secretary:
Dewayne Hendricks, WA8DZP
WA8DZP @ K3MC

Treasurer:
Patrick Mulrooney, N6QMY
N6QMY @ N6QMY

Newsletter Editor:
Steve Harding, KA6ETB
KA6ETB @ N6LDL

Frequency Coordinator:
Roy Engehausen, AA4RE
AA4RE @ AA4RE

Education Coordinator:
Larry Kenney, WB9LOZ
WB9LOZ @ W6PW

What is NCPA?

NCPA, the Northern California Packet Association, is an organization formed to foster the Digital Communications modes of Amateur Radio. So far, we have defined our goals as:

- **Education**
- **Coordination**

Education means making information available about various Digital modes, and this newsletter is but one part of that education process.

Coordination activities include frequency coordination (NCPA is recognized by NARCC as the official packet radio frequency coordinator) as well as coordinating people and their various uses of packet radio, be they DX Cluster, BBS, TCP/IP, keyboard-to-keyboard, NET/ROM, Traffic/NTS, Emergency uses of packet, or even experimenting with new frontiers of various digital modes.

We in NCPA believe that the next revolution in Ham Radio will come about in Digital Communications Technology, and in the beneficial coordination among all users of ham Digital Communications Technologies.

We invite you to join NCPA! Become part of the most dynamic group of packet folks in Northern California!

NCPA *Downlink*

Northern California Packet Association
6680B Alhambra Ave. Suite 111
Martinez, CA 94553

First Class Mail