TAP

The Hobbyist's Newsletter for
the Communications Revolution

November 1983 Issue 88

TELECOM '83 - TECHNO TOYLAND!

by Cheshire Catalyst

October 26th began the biggest, greatest, and most technologically advanced trade show in telecommunications history. The Telecom series of conferernces began in 1971 when the International Telecommunications Union (ITU) decided that the international telecommunications community needed a trade show which could bring together the world's telecom manufacturers and the international telecom network managers who bought the equipment. The ITU is the United Nations specialized agency which boils out agreement of international communications standards through its sub-entities of the Consultative Committee for International Radio (CCIR) and the Consultative Committee for International Telephones and Telegraph (CCITT).

Telecom '83 was held in the new Palais des Exposition across the main highway from Geneva Switzerland's Cointrou Airport. The exposition filled the four main halls, and spilled out onto the outdoor roof of the multi story parking garage. This outdoor area was filled with satellite earth station antennas of every decryption, from multi horn toroids, to mushroom shaped radomes containing the self stabilizing antennas used aboard rolling and pitching ships at sea when communicating via Inmarsat, the system which has now replaced the outdated Marisat, or Maritime Communications Satellite. It also held the spillover of the French Pavilion which was to small to accommodate all the French company's exhibits.

Besides the major manufacturers, a number of international Short Wave Radio stations were represented. The European DX Council, PO Box 4, St Ives, Huntington, England PE17 4FE, is a club of short wave listeners around the world. DX is the abbreviation meaning "Distant Xmission". Briefly, SWL's (Short Wave Listeners) DX (listen to distant transmissions). Let's face it, we computer types got "initial mania" from our ham radio buddies. Radio Nederlands, Radio Canada International, Radio Switzerland, and Radio Sweden had a booth together displaying the types of small portable shortwave radios which are making this hobby popular again. While many of the shortwave radios sold today are of the "Street Box" type of "Let's be cool by blasting out the neighborhood" which is bought just because it has alot of fancy buttons that never get used, the letters recieved by these shortwave stations show that there is a definite increase of shortwave listening around the globe. Many people listen to the news broadcasts of other countries, so as not to be "locked in" to the news as put forward by their own government. Which reminds me that the Voice of America was also an exhibitor in the "Shortwave Pavilion", near the booths of Radio Pieking, and the BBC.

In the USA pavilion, I spoke with one British chap who staffs the London office of an American based multi-national company, and he told me the story of British Telecom, who was showing off a brand new computer on live BBC television. When they went to log in, the screen typed back, "sorry, I got here first and changed your password. Here's a little poem to pass the time, though." The British hacker had then typed in the first two verses of my song, The Hackers Anthem (see issue 87) which he must have gotten from Newsweek (and which Newsweek got from me, the author).

The High Tech goodies included totally digital central offices, rural telephony links via radio, advanced telex machine that print English and Arabic characters, and ISDN (Integrated Services Digital Network) control switches which mix telex, data, and packet switched services.

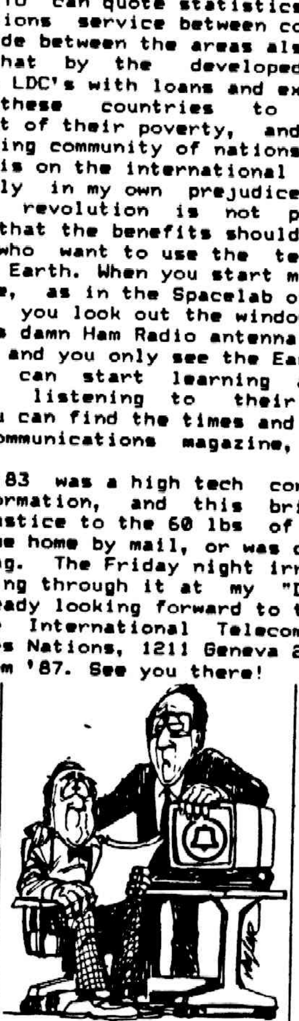
Among these exhibits were a complete international shortwave radio station operated by the International Red Cross. The invasion of Granada was underway then, and two Red Cross volunteer radio operator were chosen from those operating at the Telecom exhibit, and sent to Barbados. The major criterion as to who was chosen, was basically, who had the time from work, and no other immediate commitments so they could take off within 12 hours. It all is based on being in the right place at the right time with the right skills.

I'm afraid, as I read this over, that I have outlined Shortwave Radio as being of the most interest. Although there were French terminals with games that needed their "Smart Card" or "Credit Card with a Chip" which they passed out like candy, and television transmission studios to watch yourself freeze framed on 23 video monitors, and fiber optic transmission cables, and satellite transmission station salesmen everywhere, you have to realize that even the satellites are using radio, and very simple radio techniques at that, to bring the new level of sophisticated digital telecommunications services to most of the world. Future communications engineers will still be those people who learned Morse Code and pounded enough brass to get their Ham Radio ticket (license).

One booth that attracted my attention was set up by the ITU itself, and was staffed with personnel from the Technical Cooperation department of the ITU. The booth had panels displaying the GNP's of various "Less Developed Countries", and the amount spent on telecommunications, and forcasts of predicted telecom growth in those countries. The ITU was trying to attract development funds from the developed countries to help the LDC's bring modern communications to these countries. These folks are not trying to put a telephone in every home, because the people in those countries can't afford it, but they are trying to bring telecommunications to the rural areas in government offices, and primarily for coordination of trade. The ITU can quote statistics that when telecommunications service between countries was enhanced, trade between the areas also increased. They hope that by the developed countries supporting the LDC's with loans and expertise, it will help these countries to "bootstrap" themselves out of their poverty, and bring them into the "trading community of nations".

My emphasis on the international view here is based primarily in my own prejudices that the technological revolution is not political in nature, and that the benefits should be spread among those who want to use the technology to better life on Earth. When you start manufacturing in outer space, as in the Spacelab on board the Space Shuttle, you look out the window (when Owen hasn't got his damn Ham Radio antenna cluttering up the window) and you only see the Earth; not the borders. You can start learning about other countries by listening to their shortwave broadcasts. You can find the times and frequencies in Popular Communications magazine, and World Radio Guide.

Telecom '83 was a high tech cornocopia of technical information, and this brief article doesn't do justice to the 60 lbs of literature that followed me home by mail, or was dragged home in my duffle bag. The Friday night irregulars had their fun pawing through it at my "De-briefing" party. I'm already looking forward to the information from the International Telecommunications Union (Place des Nations, 1211 Geneva 20, Switzerland) on Telecom '87. See you there!



"Sorry, Fred, it was a choice. The computer still has expansion capabilities you're running at full potential!"

Phreaking with the TI-99/4A

by the New England Archivist

I've just purchased a TI-99/4A for purposes of boxing, and have a few words to say to anybody intending to do the same. First of all, I haven't had a chance to try it for anything so far except as an automatic dialer, but it shouuld work okay for other stuff as well. The TI-99/4A can play up to three tones plus a fourth noise tone simultaneously. The frequencies of the tones are specified to the nearest hertz and the duration to the nearest millisecond. The responses I got were pretty close on mine below about 10kHz, and below about 3kHz the frequencies were always within 10 Hz. Here's a list of some of the frequencies I've tested:

What I Wanted	What I Got	
110	110.0	(The lowest possible frequency)
697	699.1	
700	699.1	
852	853.9	
900	902.1	
941	940.0	
1000	998.7	
1100	1096.7	
1200	1202.8	
1209	1202.8	
1210	1215.9	
1300	1300.7	
1336	1331.6	
1477	1471.8	
1500	1491.5	
1633	1645.0	
1700	1694.9	
2000	1997.5	
2200	2193.4	
2600	2601.4	
3200	3995.0	
44,733	37.286.6	(The highest possible frequency)

The sounds are generated by a CALL SOUND routine call. A CALL SOUND routine call takes about 34 milliseconds to get going. Since the pulses for a quarter in a red box should be 35ms on, 35 off five times, then by leaving a 34ms space in between pulses we can excecute the followind program:

```
10 FOR I=1 TO 5
20 CALL SOUND(35,1700,0,2200,0)
30 NEXT I
```

The 35 is the duration in milliseconds, 1700 and 2200 the two frequencies, and the zeroes are the volumes for each tone (0 is the loudest volume, 30 the quietest). For auto-dialling, a duration of 100 milliseconds seems to work well.

The audio output is across 2 of the pins going into the modulator; as you're looking at the back of the TI where the modulator plugs in, the audio output is in the pin at 9 o'clock and the audio ground is the pin below that. TI sells a $20.00 headphone adapter to let you listen to this, but you can build the thing yourself for a little over $3.00 with a couple of 5-pin DIN plugs (one male, one female) at Radio Shack, hooking up the audio output leads to a headphone jack or whatever.

Looking at the wave it put out on an oscilloscope, I saw that it puts out a very square wave with voltage spikes whenever the wave shifted from a low to high state or high to low. After sticking a .27mfd capacitor across the audio leads, however, I got a very triangular wave that looks like it'll produce sounds up to about 4kHz without too much attenuation, with no harmonics. The frequency measurements were made with the capacitor and jacks hooked up as described.

So far I've been dialing by coupling a speaker from the computer to a handset. I'm trying to put together some simple sort of direct coupling with the telephone line now, and am interested in anyone else doing anything with the TI.

HIGHWAY RADAR JAMMING

Most drivers wanting to make better time on the open road will arm themselves with an expensive radar detector. However this device will not work against a gun type radar unit in which the radar signal is not present untill the cop has your car in his sights and pulls the triggeer. Then it is too late to slow down.

A better method is to continously jam any signal with a radar signal of your own. I have tested this idea with the cooperation of a local cop and found that his unit reads random numbers when our car approached him. It is suprisingly easy to make a low power radar transmitter. A nifty little semiconductor called a Gunn diode will generate microwaves when supplied with 5 to 10 vdc and enclosed in the correct size cavity (resonator). An 8 volt 3 terminal regulator can be used to get this voltage from a car's system. However the correct construction and tuning of the cavity is difficult without good microwave measurement equipment. Police radars commonly operate on the K band at 22 ghz. or more often on the X band at 10.525 ghz. Most microwave intruder alarms and motion detectors(mounted over automatic doors in supermarkets, etc.) contain a Gunn type transmitter/reciever combination that transmits about 10 milliwatts at 10.525 ghz. These units work perfectly as jammers. If you can't get one locally write to Microwave Associates in Burlington, Mass. and ask for info on "Gunnplexers" for ham radio use. When you get the unit it may be mounted in a plastic box on the dash or in a weatherproof enclosure behind the plastic grille. Switch on the power when on the open highway. The unit will not jam radar to the side or behind the car so don't go speeding past the radar trap.

An interesting phenomena you will notice is that drivers in front of you who are using detectors will hit their brakes as you approach large metal signs or bridges. Your signal is bouncing off these objects and triggering their detectors.

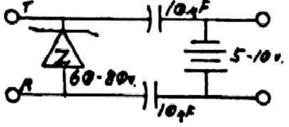
Have fun... Ben Piper

Black Boxing Update

by The Stainless Steal Rat

Recently, I moved to a new city and all my old phriends called me and ended up with a large phone bill. Since not many of my phriends had touch-tone phones or dialer pads I couldn't tell them to go and use a SCC. So I went through all my back issues of TAP and found a set of black box plans.

After a bit of experimentation I came up with a box that produces such good quality sound reproduction that you can't tell you are using a box at all. So here goes with the schematic...



As an added bonus here is how you can ring extra phones without them knowing you have one or more on the line. All you have to do is find a 55 to 90 volt transient protector (Bell makes one that fits this catagory...) and connect it in series with the ringer of the offending phone. Make sure that it has a very small capacitance below its rated voltage. 10 to 50 pf is ok. now when Bell sends a pulse of DC down your line to see how many ringers you have the protector will stay inactive and hide all your illegal ringers. However when the 90 volt ringing current comes along the protector activates and lets the current through and your phones ring !

Soon to cum: A special report on the new all electronic payphone.

Yours with a smile,
The Stainless Steal Rat

The Old Gray Faire,
She Ain't What She Used To Be.

by Cheshire Catalyst

The West Coast Computer Faire carries on a fine old tradition in computer hobbyist circles. The tradition was started in Trenton NJ in 1976 when the Trenton State College held the First Trenton Computer Festival. The Atlantic City Computer Show opened a few months later, and the Homebrew Computer Club in Sunnyvale was stirring up a hornets nest that would eventually bring us Apple Computers, software trading, and the West Coast Computer Faire. Trenton still carries on the tradition started by then Electrical Engineering Professor Sol Libes those many years ago. The Atlantic City show moved to Philadelphia, and slid into oblivion. But the premier hobbyist show is the one that grew out of the Semiconductor Valley that we lovingly call Silicon Gultch.

I've been to every West Coast Computer Faire they've held in the San Francisco area. It is now held in March of each year, and the flavor of it has changed so much, that I'm not sure I'm going back next year. The show has been getting more and more commercial with each passing year, to the point where Jim Warren, who put on these shindigs, is getting out of the game in favor of getting back into computers.

There are still bargains to be found, and the mob of people still contains a few phreaks or two among the hackers. Each year we seem to run into each other. It used to be that we would gather at the refreshment area in Brooks Hall at 4PM each day of the show, and sit and discuss what was new at the show, and in phreaking/hacking.

The show has gotten so big, that all the available space is given up to money generating booths, and places to enjoy refreshments are left to the various snack bars, but mostly to the restaurants nearby the San Francisco Civic Center. It wound up that we got together in the balcony of the main Civic Center hall. If I get there again next year, look for me in Section 212 (I'm from New York, after all, and the section numbers don't get as high as 415, to honor my hosts). The gathering will be at 4PM, as usual, but don't expect anything formal. TAP gatherings, both at the Faire, and at our Friday nite watering hole, are informal rap sessions, usually with as many as 5 conversations going on at once. Information sharing is more than swapping data on the ARPA net, you know.

Q: How many programmers does it take to change a light blub? A: None - That's a hardware problem.

Q: How many Computer repairmen does it take to change a light bulb? A: Their diagnostic ran fine, so it must be a software problem.

HOW TO WRITE FOR TAP

by Cheshire Catalyst

As I try to paste up another issue of this rag, I find that I have very little worth pasting up. Now some of it is that I can't find some of the things that have been submitted, but mostly, I can't find those little filler items that use up those extra couple of inches that are needed to fill out the botom.

If you want to write something for TAP, then set the margins on your typewriter to 45 (in case you need to hit "margin release") or set your word processor to 50 characters per line, and start typing. There are about 95 lines per column, so as it comes off your printer, you'll be able to figure out how I'm going to paste it up. One recent article would have been great, if the author hadn't put a blank line between each paragraph. We want to fill space, but I want to try to keep it to even columns, too. Right now, I'm writing this article just to fill 6 inches of space. Hmm, that's 6 lines/inch times 6 inches, so this needs to be 36 lines long (with headlines).

The thing you must remember is, by corresponding with us, you become a "correspondent". The term derives from the days when writers for a newspapers were people on trips abroad who wrote long, descriptive letters to their friends back home. Their friend's had the letters published in local newspapers (those old guys had space to try & fill, too). This newsletter is an amateur publication (you may have noticed). This means we accept manuscripts (articles) from fellow amateurs. Keep 'em coming gang!

Dealing with the Rate & Route Operator

by Fred Steinbeck

It seems that fewer and fewer people have blue boxes these days, and that is really too bad. Blue boxes, while not all that great for making free calls (since TPC can tell when the call was made, as well as where it was to and from), are really a lot of fun to play with. Short of becoming a real live TSPS operator, they are about the only way you can really play with the network.

For the few of you with blue boxes, here are some phrases which may make life easier when dealing with rate & route (R&R) operators. To get the R&R op, you send KP + 141 + ST. In some areas you may need to put another NPA before the 141 (i.e., KP + 213 + 141 + ST), if you have no local R&R ops.

The R&R operator has a myriad of information, and all it takes to get this data is mumbling cryptic phrases at her. There are basically four special phrases to give to R&R ops. They are **numbers** route, **directory** route, **operator** route, and **place name**.

To get an area code for a city, one can call the R&R operator and ask for the numbers route. For example, to find the area code for Carson City, Nevada, we'd ask the R&R op for "Carson City, Nevada, numbers route, please." and get the answer, "Right... 702 plus." meaning that 702 plus 7 digits gets us there.

Sometimes directory assistance isn't just NPA + 131. The way to get these routings is to call R&R and ask for, "Anaheim, California, directory route, *please*." Of course, she'd tell us it was 714 plus, which means 714 + 131 gets us the D.A. op there. This is sort of a pointless example, but I couldn't come up with a better one on short notice.

Let's say you wanted to find out how to get to the inward operator for Sacramento, California. The first six digits of a number in that city will be required (the NPA and an NNX). For example, let us use 916 756. We would call R&R, and when the operator answered, say, "916 756, operator route, please." The operator would say, "916 plus 001 plus." This means that 916 + 001 + 121 will get you the inward operator for Sacramento.

Do you know the city which corresponds to 503 640? The R&R operator does, and will tell you that it is Hillsboro, Oregon, if you sweetly ask for "Place name, 503 640, please."

None of this is really spectacular. However, R&R can also give information on international calls in much the same manner. And it is in these cases that the various routings becomes useful.

For example, let's say you need the directory route for Sveg, Sweden. Simply call R&R, and ask for, "International, Baden, Switzerland. TSPS directory route, please." In response to this, you'd get, "Right... Directory to Sveg, Sweden. Country code 46 plus 1170." So you'd route yourself to an international sender, and send 46 + 1170 to get the D.A. operator in Sweden.

If you need to know how to complete a call to an overseas number (that is, you need the country and city code), you can ask for, "International, Cortona, Italy, TSPS numbers route, please." and get the answer, "Right... Country code 39 plus 575 plus." This means, of course, that the city code is 575, and the plus on the end means you'd tack on the phone number there.

Inward operator routings to various countries are obtained the same way - "International, London, *England*, TSPS inward route, please." and get "Country code 44 plus 121." Therefore, 44 plus 121 gets you inward for London.

Inwards can get you language assistance if you don't speak the language. Tell the foreign inward, "United States calling. Language assistance in completing a call to (called party) at (called number)."

R&R operators are people too, y'know. So always be polite, make good use of 'em, and dial with care.

Verification

by Fred Steinbeck

There has been a great deal of controversy in the realm of phreakdom over a mysterious subject known under a number of different names, including "verification", "autoverification", "verify", "autoverify", "verify busy", and even "VFY BY". All of these names basically mean the same thing: the ability to listen to another person's telephone line from any telephone in the direct-dialable world.

Needless to say, the Bell System is very tight lipped about knowledge regarding verification. Indeed, the infamous book **Notes On Distance Dialing** ('68 edition) says, "Care must be taken to insure that the customer never gains verification capabilities." With a printed policy like that, you can imagine what their real-world policy is like! Even their own rate and route operators will not give verification routing codes (at least in my experience), one even responding, "What?! You must be crazy! We don't give those out!"

Before you get too far into this article, I will state simply: I don't know how to verify. However, I have been fooling with various things related to it, and collecting information on it for some time now. Therefore, while I can't do it (yet), I may be able to point some other bright **TAP**per on the right track, and perhaps he or she will show us all how. If you have knowledge not covered in this article, but don't want to write an article on your own, please send your ideas, comments, or information to **Project Verify, c/o TAP**.

Verify has also been called "autoverify", and I have no idea why. This is not, to my knowledge, a Bell System term (at least I've never seen it in any manuals). As far as I know, there is verify, which means being able to listen to speech (kind of; see below) on a line, and there is the "emergency interrupt" which allows you to take part in the conversation taking place on the line in question. It has been suggested that "autoverify" is the same as an emergency interrupt, but I tend to disagree with this idea.It should be noted that the verification circuitry does not actually let an operator listen to a conversation without making a beep on the line every so often. Instead, she will hear encrypted speech. However, I believe with the proper methods, verify can be converted to an emergency interrupt.

Verification is normally done either by your normal "0" (TSPS) operator, if the call is in your home NPA (HNPA), or by an inward operator (IO). If the call is outside your HNPA, your normal operator will call the IO for the NPA, and say, "Verify busy (or "Emergency interrupt") please, 555-1212." The IO will then perform whatever magic he or she must, and then report back. If the call is in your HNPA, though, the "0" operator can do the verification himself by using the "VFY BY" key on her keyshelf. However, in some areas, the operator uses a routing code to accomplish verification, and this is the loop hole we shall attack.

It follows that if a IO or "0" operator can do it, so can we, with a blue box. Now, courtesy of Robert Allen (who brought it to my attention) and Susan Thunder (who apparently discovered it), here is what used to work for getting operators to hook you into a conversation with other people (i.e., let you listen to them until you hung up): You'd call the operator and say, "Operator, TSPS Maintenance Engineer calling. Ring forward to 001 + NPA + 7D, ring back to my number, hit ring forward, no AMA, and then position release."

This creates some problems, and you must be familiar with TSPS to understand them. When you call into a TSPS console (by dialing "0"), you are on the "back", or incoming part of a loop. When she places a call for you, the call goes out on the "forward", or outgoing part of the loop. If an operator wants to make a call, she punches KP FWD (keypulse forward), the number, and ST. RING FWD puts a 90 volt ringing signal across the forward part of the line (and **may** dial the number as well). The problem arises from the fact that I don't know if RING FWD will actually dial a call, and if there is some other subtle difference between it an KP FWD.

Let us assume ringing forward makes a call from the TSPS console to whatever number is given. Ring back causes your phone to ring (it is assumed you hung up after giving her your instructions; if you didn't, you'd hear an annoying 90 volts across the earpiece...) "No AMA" means "no automatic message accounting", so nobody gets billed for the call, although it will show up on a tape somewhere. "Position release" removes the operator from the circuit, and allows her to receive other calls. This leaves an unaccounted-for ring forward.

The verification circuit, as you know, likes to encrypt conversation, which is something we don't want. Well, the second RING FWD sends another 90 volts crashing against the verify circuitry, which Judas Gerard thinks removes the voice encryption from the line, puts the operator (and you) in circuit, and puts a beep tone on the line every five seconds. This seems to make sense, and I am inclined to agree with him.

The bit about "...001 + NPA + 7D" causes the thought "MF routing code" to spring immediately to mind. Now, the above trick was supposed to work in the 213 NPA. I have tried both "KP + 001 + 213 + 7D + ST", and some other area codes. I generally get nothing, a reorder signal, or a tandem recording.

Here's some food for thought: On an official Telco sheet I have, labeled "213 NPA MF Routing Codes", 001 is listed as "VFY BY", or verify busy for the 213 NPA. 002 is listed for the 805 NPA. Ma Bell likes to have standardized routing codes, such as 121 for inward, 131 for DA, etc. It would seem logical, then, that 001 would be a sort of "standard" verify code, and other prefixes would be tacked on at 002, 003, etc. However, I have heard from a retired operator that verification codes are different from area to area, and are not always nice numbers like 001 or 002. Ah, well, a guy can hope, can't he?

Some suggestions for future attacks on this dilemma: Everyone call your operators and subtley ask questions. I have found they tend to give information out easier if you ask for something that you would ordinarily have to be a company employee to know about, such as rate steps, operator routings, etc. Casually let slip that you used to be (or still are) an operator, or that you work for company security. Also, you might want to blue box some codes like 001 followed by your NPA and the last 7D of a busy number. If you get a sort of "whispery noise", try blasting the line with a ringing signal (you might piggyback another line onto yours and call the piggyback to generate the 90 volts) and see if that does anything. Don't forget to send in any scraps of info, no matter how mundane, to **Project Verify, c/o TAP**.

T A P
TECHNOLOGICAL ASSISTANCE PROGRAM
Room 603, 147 West 42 St, New York City, 10036

Back Issues are $.75 each. Issue #50 is $1.50.
Subscriptions - 10 issues per year - $10.
Foreign Air Mail - $13 in Money Order drawn on a US Bank. Sample - 3 International Reply Coupons.

PUBLISHED FOR INFORMATIONAL
PURPOSES ONLY SINCE 1971

ANNEE MONDIALE DES COMMUNICATIONS
WORLD COMMUNICATIONS YEAR
AÑO MUNDIAL DE LAS COMUNICACIONES
1983