October 26th began the biggest, greatest, and most technologically advanced trade show in telecommunications history, Telecom '83. The conference 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 telecommunications manufacturers and the international telecom network managers who bought the equipment. The ITU, the United Nations specialized agency which sets the international communications standards through its sub-entities of the Consultative Committee for International Radiocommunications (CCIR) and the Consultative Committee for International Telecommunications 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 outdoors of the multi-story parking garage. This outdoor area was filled with satellite earth station antennas of every description, from multi horn toroids, to mushroom shaped radomes containing the self stabilizing antennas used aboard rolling and pitching ships at sea. The technology is used aboard rolling and pitching ships at sea when communicating via Inmarsat, the system which has now replaced the outdated Marisat, or Maritime Communications Satellite.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 spill-over of the French Pavilion which was too small to accommodate all the French company's exhibits.

Besides the major manufacturers, a number of international Short Wave Radio stations were also represented. The European DX Council, PO Box 4 SE-1, Ives, Huntington, England PE17 4FE, is a club of short wave listeners around the world. DX is the abbreviation meaning "Distance Transmission". British 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 short wave radios which are making this hobby popular again. While many of the short wave radios sold today are of the "Street Box" type of "Let's be done with this nonsense from our own radio buddies. These radios were small, portable, and meant to be listened to in the outdoors or while walking. Many people listen to the news broadcasts around the world, so as not to be "locked in" to the news as put forward by their own government. Which radio's said, "Sorry. Fred. I was & chose. The computer still has expansion capabilities you're looking for right now." The British hacker had then typed in the first two verses of "Ode to a Less Developed Country". The Hackers Anthem (see issue 87) which he must have gotten from Newsweek (and which Newsweek got from me, the author). The English translator explained 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. The future telecommunications engineers will still be the people who learned Morse Code and pounded enough keys 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 forecasts of predicted telecom growth in these 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 there 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 them increased. They hope that by the developed countries supporting the LDC's with loans and expertise, it will help them 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 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. If you start manufacturing in outer space as in the Space Lab on board the Space Shuttle, you look out the window when Owen White got his first 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 short wave broadcasts. You can find the times and frequencies in Popular Communications magazine, and World Radio Guide.

Telecom '83 was a high tech cornucopia of technical information, and the 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 party through it too 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!
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 caller, but it should 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:

<table>
<thead>
<tr>
<th>What I Wanted</th>
<th>What I Got</th>
</tr>
</thead>
<tbody>
<tr>
<td>110</td>
<td>110.0 (The lowest possible frequency)</td>
</tr>
<tr>
<td>697</td>
<td>699.1</td>
</tr>
<tr>
<td>700</td>
<td>699.1</td>
</tr>
<tr>
<td>802</td>
<td>805.3</td>
</tr>
<tr>
<td>900</td>
<td>902.1</td>
</tr>
<tr>
<td>941</td>
<td>940.8</td>
</tr>
<tr>
<td>1000</td>
<td>998.7</td>
</tr>
<tr>
<td>1090</td>
<td>1095.7</td>
</tr>
<tr>
<td>1200</td>
<td>1208.2</td>
</tr>
<tr>
<td>1210</td>
<td>1208.6</td>
</tr>
<tr>
<td>1300</td>
<td>1315.2</td>
</tr>
<tr>
<td>1477</td>
<td>1471.6</td>
</tr>
<tr>
<td>1500</td>
<td>1491.5</td>
</tr>
<tr>
<td>1633</td>
<td>1645.0</td>
</tr>
<tr>
<td>1700</td>
<td>1694.9</td>
</tr>
<tr>
<td>1800</td>
<td>1797.9</td>
</tr>
<tr>
<td>2000</td>
<td>2195.4</td>
</tr>
<tr>
<td>2600</td>
<td>2681.4</td>
</tr>
<tr>
<td>3200</td>
<td>3295.0</td>
</tr>
<tr>
<td>44,733</td>
<td>37,286.6 (The highest possible frequency)</td>
</tr>
</tbody>
</table>

The sounds are generated by a CALL BOUND routine call. A CALL BOUND 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 execute the followind program:

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

The 35 is the duration in milliseconds, 1700 and 2200 the two frequencies, and the zeros are the voltage spikes. So I got a very clean tone (6 is the loudest volume, 38 the quietest). For auto-dialling, a pulse 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 execute the followind program:

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

On the other hand, 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.

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 and mine was a dial phone (with the 90 volt ringing current), I had to tell them to go and use a SCC. So I bought 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 transistor. However (this makes one that fits this category...) 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. 1Ko 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 sum: A special report on the new all electronic payphone.

Yours with a smile,
The Stainless Steal Rat
Dealing with the Rate & Route Operator
by Fred Steinbeck

It seems that fewer and fewer people have blue boxes these days, and it is really too bad. Blue boxes, while not all that great for long distance calls (since TPC called 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 before the 141 (i.e., KP + 213 + 141 + BT). If you have no local R&R ops.

The R&R operator has a myriad of information, and all it takes is to give special phrases to get to R&R ops. They have numbers route, directory route, operator route, and place name.

To get an area code for a city, you need to call the R&R operator and ask for, "Anahiem, California, directory route, please." Of course, she'd tell us it was 714, 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 NXX). 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 then say, "916 plus 001 are you." 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 inquiry, the operator answered, say, "816 756, operator route, please." The operator would then say, "816 plus 001 are you." This means that 816 + 001 + 121 will get you the inward operator for Sveg.

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, "Country, Cortina, Italy, TSPS numbers route, please." And 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." In response to this inquiry, the operator answered, say, "816 756, 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 variety of 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 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 TAPper on the right track, and perhaps he or she will show us all how.

If you have knowledge not covered in this article, but you don't want to write an article on your own, please send your ideas, comments, or information to Project Verify, c/o TAP.

Verification 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 verification 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" or "O" (TSPS) operator. The operator is in your home NPA (HNPA), or by an inward operator. If the call is outside your HNPA, your normal operator will give the IO for the HNPA, 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 "O" operator can do the verification himself by using the "VFY BY" key on her keyset. 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 10 or "O" 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 up to a conversation taking place on the line. If you let them listen to them until you hung up) You'd call the operator and say, "Operator, TSPA Maintenance Engineer calling. Ring forward to 001 + NPA + 7D, ring No. to my number, hit ring forward, no AMA, and then position release." This creates some problems, and you must be familiar with TSPA to understand them. When you call into a TSPA 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 the "forward", or outgoing part of the loop. If an operator wants to make a call, she punches KP FWD (for "key pad forward", the key "K") 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 and KP FWD.

Let us assume ringing forward makes a call from the TSPA 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 Gerad 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 for the 213 NPA. 002 is listed for the 805 NPA. Ma Bell likes to have standardized routing codes, such as 121 for inward, 121 for out, 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 subtly 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 that verification code 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 — $12. Foreign Air Mail - $13 in Money Order drawn on a US Bank. Samples - 3 International Reply Coupons.

PUBLISHED FOR INFORMATIONAL PURPOSES ONLY SINCE 1971