

TELCOM7.TXT

Extracting [Basic7.doc] ...

=====
=BASIC TELECOMMUNICATIONS=
=====

Part VII

Preface:

After most neophyte phreaks overcome their fascination with Metro codes and WATS extenders, they will usually seek to explore other avenues in the vast phone network. Often they will come across references such as "simply dial KP + 2130801050 + ST for the Alliance teleconferencing system in LA." Numbers such as the one above were intended to be used with a blue box; this article will explain the fundamental principles of the fine art of blue boxing.

Genesis:

In the beginning, all long distance calls were connected manually by operators who passed on the called number verbally to other operators in series. This is because pulse (aka rotary) digits are created by causing breaks in the DC current (see Basic Telcom V). Since long distance calls require routing through various switching equipment and AC voice amplifiers, pulse dialing cannot be used to send the destination number to the end local office (CO).

Eventually, the demand for faster and more efficient long distance (LD) service caused Bell to make a multi-billion dollar decision. They had to create a signaling system that could be used on the LD Network. Basically, they had two options:

[1] To send all the signaling and supervisory information (ie, ON & OFF HOOK) over separate data links. This type of signaling is referred to as out-of-band signaling.

-or-

[2] To send all the signaling information along with the conversation using tones to represent digits. This type of signaling is referred to as in-band signaling.

Being the cheap bastard that they naturally are, Bell chose the latter (and cheaper) method -- IN-BAND signaling. They eventually regretted this, though (heh, heh)...

IN-BAND SIGNALING PRINCIPLES:

TELCOM7.TXT

When a subscriber dials a telephone number, whether in rotary or touch-tone (aka DTMF), the equipment in the CO interprets the digits and looks for a convenient trunk line to send the call on its way. In the case of a local call, it will probably be sent via an inter-office trunk; otherwise, it will be sent to a toll office (class 4 or higher -- see Telcom IV) to be processed.

When trunks are not being used there is a 2600 Hz tone on the line; thus, to find a free trunk, the CO equipment simply checks for the presence of 2600 Hz. If it doesn't find a free trunk the customer will receive a re-order signal (120 IPM busy signal) or the "all circuits are busy..." message. If it does find a free trunk it "seizes" it -- removing the 2600 Hz. It then sends the called number or a special routing code to the other end or toll office.

The tones it uses to send this information are called multi-frequency (MF) tones. An MF tone consists of two tones from a set of six master tones which are combined to produce 12 separate tones. You can sometimes hear these tones in the background when you make a call but they are usually filtered out so your delicate ears cannot hear them. These are NOT the same as touch-tones.

To notify the equipment at the far end of the trunk that it is about to receive routing information, the originating end first sends a Key Pulse (KP) tone. At the end of sending the digits, the originating end then sends a Start (ST) tone. Thus to call 914-359-1517, the equipment would send KP + 9143591517 + ST in MF tones. When the customer hangs up, 2600 Hz is once again sent to signify a disconnect to the distant end.

History:

In the November 1960 issue of The Bell System Technical Journal, an article entitled "Signaling Systems for Control of Telephone Switching" was published. This journal, which was sent to most university libraries, happened to contain the actual MF tones used in signaling. They appeared as follows:

Digit	Tones
-----	-----
1	700 + 900 Hz
2	700 + 1100 Hz
3	900 + 1100 Hz
4	700 + 1300 Hz
5	900 + 1300 Hz
6	1100 + 1300 Hz
7	700 + 1500 Hz
8	900 + 1500 Hz
9	1100 + 1500 Hz
0	1300 + 1500 Hz

TELCOM7.TXT

KP 1100 + 1700 Hz
ST 1500 + 1700 Hz
11 (*) 700 + 1700 Hz
12 (*) 900 + 1700 Hz
KP2 (*) 1300 + 1700 Hz

(*) Used only on CCITT SYSTEM 5 for special international calling.

Bell caught wind of blue boxing in 1961 when it caught a Washington state college student using one. They originally found out about blue boxes through police raids and informants. In 1964, Bell Labs came up with scanning equipment, which recorded all suspicious calls, to detect blue box usage. These units were installed in CO's where major toll fraud existed. AT&T Security would then listen to the tapes to see if any toll fraud was actually committed. Over 200 convictions resulted from the project. Surprisingly enough, blue boxing is not solely limited to the electronics enthusiast; AT&T has caught businessmen, film stars, doctors, lawyers, college students, high school students and even a millionaire financier (Bernard Cornfeld) using the device. AT&T also said that nearly half of those that they catch are businessmen.

Of course, phone phreaks have achieved an almost cult status. They have also had their fair share of media. In October 1971, Esquire published the infamous "Secrets of the Little Blue Box" article which featured phreaks such as Captain Crunch, who took his name from the cereal which one gave away whistles that produced a perfect 2600 Hz pitch; Joe Engressia, the blind phreak; and Mark Bernay, one of the nation's first and oldest phreaks. Others such as Apple computer co-founders Steve Wozniak & Steve Jobs have also had blue box backgrounds. 1971 also saw the publication of the first issue of YIPL, the phone phreak newsletter, (now TAP) under the editorship of supreme yippie Abbie Hoffman.

Usage:

To use a blue box, one would usually make a free call to any 800 number or distant directory assistance (NPA-555- 1212). This, of course, is legitimate. When the call is answered, one would then swiftly press the button that would send 2600 Hz down the line. This has the effect of making the distant CO equipment think that the call was terminated and it leaves the trunk hanging. Now, the user has about 10 seconds to enter in the telephone number he wished to dial -- in MF, that is. The CO equipment merely assumes that this came from another office and it will happily process the call. Since there are no records (except on toll fraud detection devices!) of these MF tones, the user is not billed for the call. When the user hangs up, the CO equipment simply records that he hung up on a free call.

DETECTION:

TELCOM7.TXT

Bell has had 20 years to work on detection devices; therefore, in this day and age, they are rather well refined. Basically, the detection device will look for the presence of 2600 Hz where it does not belong. It then records the calling number and all activity after the 2600 Hz. If you happen to be at a fortress fone, though, and you make the call short, your chances of getting caught are significantly reduced (see Telcom VI). Incidentally, there have been rumors of certain test numbers (see Telcom II) that hook directly into trunks thus avoiding the need for 2600 Hz and detection!

Another way that Bell catches boxers is to examine the CAMA (Centralized Automatic Message Accounting) tapes. When you make a call, your number, the called number, and time of day are all recorded. The same thing happens when you hang up. This tape is then processed for billing purposes. Normally, all free calls are ignored. But Bell can program the billing equipment to make note of lengthy calls to directory assistance. They can then put a pen register (aka DNR) on the line or an actual full-blown tap. This detection can be avoided by making short-haul (aka local) calls to box off of.

It is interesting to note that NPA+555- 1212 originally did not return answer supervision. Thus the calls were not recorded on the AMA/CAMA tapes. AT&T changed this though for "traffic studies!"

CCIS:

Besides detection devices, Bell has begun to gradually redesign the network using out-of-band signaling. This is known as Common Channel Inter-office Signaling (CCIS). Since this signaling method sends all the signaling information over separate data lines, blue boxing is impossible under it.

While being implemented gradually, this multi-billion dollar project is still strangling the fine art of blue boxing. Of course until the project is totally complete, boxing will still be possible. It will become progressively harder to find places to box off of, though. In areas with CCIS, one must find a directory assistance office that doesn't have CCIS yet. Area codes in Canada and predominately rural states are the best bets. WATS numbers terminating in non-CCIS cities are also good prospects.

Pink Noise:

Another way that may help to avoid detection is too add some "pink noise" to the 2600 Hz tone.

Since 2600 Hz tones can be simulated in speech, the detection equipment must be careful not to misinterpret speech as a disconnect signal. Thus a virtually

pure 2600 Hz tone is required for disconnect.

Keeping this in mind, the 2600 Hz detection equipment is also probably looking for pure 2600 Hz or else it would be triggered every time someone hit that note (highest E on a piano = 2637 Hz). This is also the reason that the 2600 Hz tone must be sent rapidly; sometimes, it won't work when the operator is saying "Hello, hello." It is feasible to send some "pink noise" along with the 2600 Hz. Most of this energy should be above 3000 Hz. The pink noise won't make it into the toll network (where we want our pure 2600 Hz to hit) but it should make it past the local CO and thus the fraud detectors.

CONSTRUCTION:

While step-by-step details for the construction of a blue box is beyond the scope of this tutorial, it is worthwhile to mention some of the details.

First there are some alternatives but they are not as good as an actual blue box. Many computers are capable of generating MF tones. Thus, your local phriendly software pirate should have a program compatible for your computer.

However, it is highly advisable not to box from home as stated in The Ten Commandments (as interpreted for phreaks by Fred Steinbeck -- TAP #86).

- I. Box thou not over thine home telephone wires, for those who doest must surely bring the full wrath of the Chief Special Agent down upon thy heads.

Another alternative that has a moderate success rate involves recording the tones from a phriend with a box or computer onto a cassette tape. They can then be used at a fortress.

As for actual construction techniques, TAP has devoted many issues to blue boxing. Basically, a blue box is merely a device capable of generating two different tones simultaneously. There are two basic construction methods that I will outline below for the electronics hobbyist.

The first involves the use of two 555 timer chips (or a 556 -- i.e., two 555's in one chip). It offers excellent frequency and voltage stability. Also, it does not need a diode matrix keypad but used double-pole switches instead. Schematics for this type of box can be found in TAP issue #29.

The other common box makes use of two Intersil 8038CC Function Generators. It also requires a diode matrix keypad, potentiometers, an LM-100 voltage regulator, a 741 Op-amp, and a handful of other parts. The schematics for this type of blue box can be found in TAP #26.

Both designs draw about 20 ma of current.

TELCOM7.TXT

Also, most blue boxes use telephone earpieces (with the varistor removed) for speakers. These can be easily liberated from fortress fones with a small coping saw.

Usually, the hardest part about building a blue box is the calibration. A frequency counter is a must and an oscilloscope won't hurt.

Some boxes also take timing into account. It is feasible on the ESS systems that they check to see if the digits are of uniform length. If they aren't, they are probably from a blue box and a trouble card may be dropped. With this in mind, the Bell standard for MF pulses and interdigit intervals is around 75 ms. It varies with the equipment used since ESS can handle higher speeds and doesn't need interdigit intervals.

APPLICATIONS:

Besides dialing normal calls free, i.e., KP+NPA+NNX+XXXX+ST, blue boxes offer the entire network for exploration. Emergency break-ins, service monitoring (aka taps), stacking tandems (the art of busying out all trunks between two points), re-routing calls, conference calls, and much, much more are all feasible. Although, Bell frequently changes these codes due to phreaks.

Here are some standard ones, though:

OPERATOR & OTHER CODES:

(an optional NPA may proceed all of the numbers; otherwise, you will reach the one local for the area where the call is originated)

001 -- Trunk Access System

009 -- Rate Quote System

101 -- toll office test board

121 -- INWARD Operator

This operator assists the local "0" operator in completing calls. (S)he will do virtually anything for you providing it is within her NPA.

131 -- Operator Directory assistance

141 -- Rout & Rate

(141 defunct -- use KP + 800 + 141 + 1212 + ST)

These operators are very useful if you know how to mumble a few cryptic phrases as compiled below (with thanks to Fred Steinbeck):

To find out...

...Area Codes

For example say , "Miami, Florida, numbers route, please." The R&R operator will tell you "305 plus," meaning that 305 plus the seven digit number will get you Miami.

... Inward Operator City Codes

Usually, the INWARD operator for an area is simply KP + NPA + 121 + ST. In some area codes, though, there are several large cities and thus several inwards. To find the inward for a specific city, you would say "916 756, operator route, please" to the R&R operator who will then tell you "916 plus 001 plus." This means that KP+ 916 + 001 + 121 + ST will get you an inward for Sacramento, CA (916-756).

... City names

If you want to know the city that corresponds to an area code and exchange, you simply tell the R&R, "Place name, 914 390, please." In this example, the R&R operator will respond with "White Plains, NY."

... International Directory Assistance

If you need a directory route for London, you could say "International, London, England. TSPS directory route, please." The R&R operator will respond with "Directory to London, England. Country code 44 plus 1 plus 986 plus 3611." Therefore to get a DA operator in London, you would route yourself to an international sender and KP + 04419863611 + ST.

... Country & City codes

If you need to know the country and city code for an international number you can say "International, Sydney, Australia, TSPS numbers route, please" and get "Country code 61 plus 2."

... International Inwards Routes

To get routing codes for international inwards say "International, London, England, TSPS inward route, please." The R&R Operator will respond with "Country code 44 plus 121."

TELCOM7.TXT

Finally, to get language assistance for completing a foreign call you can tell the foreign inward, "United States calling. Language assistance in completing a call to (called party) at (called number)."

151 -- overseas incoming (212 + & 914+)

160-XX0 -- Various Overseas Operators

161 -- trouble reporting operator (defunct)

181 -- Coin Refund Operator

18X -- Overseas senders

To make an international call, one would KP + 011 + 0CC + ST where CC is the country code. This will route you to the appropriate overseas sender. You will then receive a 480 Hz dial tone. Here you enter KP + 0CC + city code + local number + ST and the call is on its way.

Country codes can be either 1, 2, or 3 digits but they must be padded for three digits to create a pseudo-country code with extra zero's if necessary. For example, England, country code 44, becomes 044.

To see which international sender a certain country (lets use French Guiana, country code 594, for example) goes through, you can dial KP + 011 + 594 + ST, wait for the Proceed to Send tone then KP + 000 + 0000 + ST and you will receive a recording saying which ISC (International Switching Center) it is. For the example it will say, "This is the international switching center in Pittsburg, PA -- This is a recording - 4121." You can actually route calls to certain senders you{self (KP + NPA + 18X + ST) but it is better off not to since it may look suspicious if a call is sent through a sender that it shouldn't go through. Here are the senders:

182 -- White Plains, NY

183 -- New York, NY

184 -- Pittsburg, PA

185 -- Orlando, FL

186 -- Oakland, CA

187 -- Denver, CO

188 -- New York, NY

Also, there tends to be alot of talk about the Code 11, Code 12, KP2, ST2, & ST2P keys. While they do exist the blue boxer need not concern himself with them. The first three are used on CCITT System 5. This is the signaling system that the International Senders use to send information to other countries. These codes are usually added iutomatically just like the language assistance digit [which distinguishes operator (or blue box) dialed

TELCOM7.TXT

calls from customer dialed calls]. The STP, ST3P, & ST2P tones are used when equipment is communicating with the TSPS. These also are automatically added when needed in most cases.

[see Telcom III for more on International Switching Centers (ISC)]

11XXX -- miscellaneous operators

11501 -- universal cordboard operator

11511 -- conference operator

11521 -- mobile operator

11531 -- marine operator

11541 -- LD incoming switchboard

11551 -- leave word for time & charges (neat stuff)

11561 -- same as 11551 but for hotel/motels

11571 -- overseas operators -- language assistance

The 11XXX series is interesting scanning material.

Miscellaneous Routing Codes :

Alliance Teleconferencing has several numbers, a few of which are listed below:

KP + 213 080 XXXX + ST

KP + 305 025 XXXX + ST

KP + 312 001 XXXX + ST

XXXX = 1050, 1100, or a few others

Also, at KP + 317 009 + ST there is a MF tone checker. After the beep-kerclunk, dial in KP + 999 1234567 890 + ST and it will repeat the digits that you pulsed if they are of the right frequency.

Tandem Scanning:

To find all sorts of interesting things, you must look. Begin scanning three digit codes in your area (i.e., KP + 000 + ST, KP + 001 + ST, etc.). Keep track of all of your results. Sometimes you must probe things, send additional digits and see what happens, send touch-tone, send it 2600 Hz, rip it apart. You never know, you may run into something phun, like a computer that checks CC numbers.

Incidentally, in some exchange you can dial inwards and other box codes directly! For example, 914-121-1111 will get you a NY inward. The only

TELCOM7.TXT

problem is that a 0 or 1 as the first digit of the exchange is usually prohibited in customer dialing. Somebody may have "accidentally" changed this screening code on your ESS's computer, though -- you never know and it can't hurt to try. WATS translation numbers also take up some of the 0XX & 1XX codes.

Finally, certain tones on the blue box can also be used for other purposes. An MF "2" corresponds to COIN COLLECT while "KP" corresponds to COIN RETURN. Thus every blue box is also a green box (see Telcom VI).

Enter [filename] or [#] to read, [D]ownload, [M]ark, [V]iew, [L]ist, or [H]elp
[45] Mins Left [# [filename] D M V L H [Return] to Quit]? Time limit exceeded!

Thank you for using AViewCom!

AViewCom is installed here on a Trial Basis
If you found this utility useful
please ask your SysOp to register it.

Press [Return] to continue?

Downloaded From P-80 International Information Systems 304-744-2253