

## TELCOM5.TXT

Extracting [Basic5.doc] ...

=====

=BASIC TELECOMMUNICATIONS=

=====

PART V

### PREFACE:

Previous installments of this series were focused on telephony from a Network point-of-view. Part V will deal with telephone electronics focusing primarily on the subscriber's telephone. Hereinafter simply referred to as "fone."

### Wiring:

-----

Assuming a standard one-line fone, there are usually 4 wires that lead out of the fone set. These are standardly colored red, green, yellow, & black. The red & green wires are the two that are actually hooked up to your CO. The yellow wire is sometimes used to ring different fones on a party line (ie, one #, several families--found primarily in rural areas where they pay less for the service and they don't use the fone as much); otherwise, the yellow is usually just ignored. On some two-line fones, the red & green wires are used for the first fone # and the yellow & black are used for the second line. In this case there must be an internal or external device that switches between the two lines and provides a hold function. (Such as Radio Shack's outrageously priced 2 line & hold module).

In telephony, the green & red wires are often referred to as tip (T) & ring (R), respectively. The tip is the more positive of the two wires. This naming goes back to the old operator cord boards where one of the wires was the tip of the plug and the other was the ring (of the barrel).

A rotary fone (aka dial or pulse) will work fine regardless of whether the red (or green) wire is connected the tip(+) or ring(-). A touch-tone (TM) fone is a different story, though. It will not work except if the tip(+) is the green wire. [Although, some of the more expensive DTMF fones do have a bridge rectifier which compensates for polarity reversal.] This is why under certain (non-digital) switching equipment you can reverse the red & green wires on a touch-tone fone and receive free DTMF service. Even though it won't break dial tone, reversing the wires on a rotary line on a digital switch will cause the tones to be generarted.

Voltages, Etc.

-----

When your telephone is on-hook (ie, hung up) there is approximately 48 volts of DC potential across the tip & ring. When the handset of a fone is lifted a few switches close which cause a loop to be connected (known as the "local loop") between your fone & the CO. Once this happens DC current is able to flow through the fone with less resistance. This causes a relay to energize which causes other CO equipment to realize that you want service. Eventually, you should end up with a dial tone. This also causes the 48 VDC to drop down into the vicinity of 12 volts. The resistance of the loop also drops below the 2500 ohm level, though FCC licensed telephone equipment must have an off-hook impedance of 600 ohms.

As of now, you ahands of our "friends" at D&B. To say the least, they weren't exactly thrilled about it. In fact, they did not even believe that they had a security problem! (Well, that just goes to prove that if you are good, no one knows that you are there!)

In a big effort to defeat us, they called in an outside service to spruce up their "security." Well, fortunately for us, we were able to find out about the new system! (Which wasn't really a problem. First, they had the new dial-ups when you logged on, and as always they have a nice little place on Telenet! (Where we do most of our work: C 20188).

Now, they have set up a new system they like to call DunsNet. They are trying to pass it off as a ectionately call this mute a black box.

The following are instructions on how to build a simple black box. Of course, anything that prevents the voltage from dropping would work.

You only need two parts: A SPST toggle switch and a 10,000 ohm (10 K), 1/2 watt resistor. Any electronics store should stock these parts.

Now, cut 2 pieces of wire (about 6 inches long) and attach one end of each wire to one of the terminals on the switch. Now turn your K500 (standard desk fone) upside down and take off the cover. Locate wire (disconnect it from its terminal). Now bring the switch out the rear of the fone and replace the cover.

Put the switch in a position where you receive a dial tone. Mark this position NORMAL. Mark the other side FREE.

When your phriends call (at a prearranged time), quickly lift & drop the receiver as fast a possible. This will stop the ringing (do it again if it doesn't) with out starting the billing. It is important that you do it quickly (less than 1 second). Then put the switch in the FREE position and pick up the fone. Keep all calls short and preferably under 15 minutes.

# TELCOM5.TXT

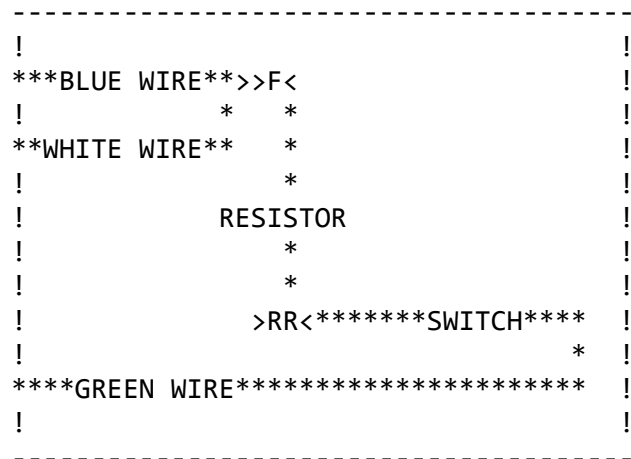
NOTE: If someone picks up an extension in the called parties house and that fone is not set for FREE then billing will start.

NOTE: An old way of signalling a phriend that you are about to call is making a collect call to a non-existant person in the house. Since your friend will not accept the charges, he will know that you are about to call and thus prepare the black box (or visa versa).

WARNING: The Telco can detect black boxes if they suspect one on your line. This is done due to the presence of AC voice signal at the wrong DC level!

Pictoral Diagram:

(Standard Rotary K500 fone)



NOTE: The Black Box will not work under ESS or other similar digital switches since ESS does not connect the voice circuits until the fone is picked up (& billing starts). Instead, ESS uses an "artificial" computer generated ring.

Ringing:

-----

To inform a subscriber of an incoming call, the Telco sends 90 volts (PK) of pulsing DC down the line (at around 15 to 60 Hz; usually 20 Hz). In most fones this causes a metal armature to be attracted alternately between two electro-magnets thus striking 2 bells. Of course, the standard bell (patented in 1878 by Tom A. Watson) can be replaced by a more modern electronic bell or signaling device.

Also, you can have lights and other similar devices in lieu of (or in conjunction with) the bell. A simple neon light (with its corresponding resistor) can simply be connected between the red & green wires (usually L1 & L2 on the network box) so that it lights up on incoming calls.

## TELCOM5.TXT

WARNING: 90 VDC can give quite a shock. Exercise extreme caution if you wish to further persue these topics.

Incidentally, the term "ring trip" refers to the CO process involved to stop the AC ringing signal when the calling fone goes off hook.

NOTE: It is suggested that you actually dissect fones to help you better understand them. It will also help you to better understand the concepts here if you actually prove them to yourself. For example, actually take the voltage readings on your fone line [any simple multi-tester (a must) will do.] Phreaking is an interactive process not a passive one!

Dialing:

-----

On a standard fone, there are two common types of dialing: pulse & DTMF. Of course, some people insist upon being different and don't use the DT thus leaving them with MF (Multi Frequency, aka operator, blue box) tones. This is another "no-no" and the Telco Security gentlemen have a special knack for dealing with such "phreaks" on the network.

When you dial rotary, you are actually rapidly breaking & reconnecting (breaking & making) the local loop once for each digit dialed. Since the physical connection must be broken, you cannot dial if another extension (of that #) is off-hook. Neither of the fones will be able to dial pulse unless the other hangs up.

Another term often referred to in telephone electronics is the break ratio. In the US, the standard is 10 pulses per second. When the circuit is opened it is called the break interval. When it is closed it is called the make interval. In the US, there is a 60 millisecond (ms) make period and a 40 ms break period. ( $60+40=100$  ms =  $1/10$  second). This is referred to as a 60% make interval. Some of the more sophisticated electronic fones can switch between a 60% & a 67% make interval. This is due to the fact that many foreign nations use a 67% break interval.

Have you ever been in an office or a similar facility and saw a fone waiting to be used for a free call but some asshole put a lock on it to prevent outgoing calls?

Well, don't fret phellow phreaks, you can simulate pulse dialing by rapidly depressing the switchhook. (If you depress it for longer than a second it will be construed as a disconnect.) By rapidly switchhooking you are causing the local loop to be broken & made similar to rotary dialing! Thus if you can manage to switchhook rapidly 10 times you can reach an operator to place any call you want! This takes alot of practice, though. You might want to

# TELCOM5.TXT

practice on your own fone dialing a friend's # or something else. Incidentally, this method will also work with DTMF fones since all DTMF lines can also handle rotary.

Another problem with pulse dialing is that it produces high-voltage spikes that make loud clicks in the earpiece and cause the bell to "tinkle." If you never noticed this then your fone has a special "anti-tinkle" & earpiece shorting circuit (most do). If you have ever dissected a rotary fone (a must for any serious phreak) you would have noticed that there are 2 sets of contact that open and close during pulsing (on the back of the rotary dial under the plastic cover). One of these actually opens and closes the loop while the other mutes the earpiece by shorting it out. The second contacts also activates a special anti-tinkle circuit that puts a 340 ohm resistor across the ringing circuit which prevents the high voltage spikes from interfering with the bell.

Dual Tone Multi Frequency (DTMF) is a modern day improvement on pulse dialing in several ways. First of all, it is more convenient for the user since it is faster and can be used for signaling after the call is completed (ie, SCC's, computers, etc.). Also, it is more up to par with modern day switching equipment (such as ESS) since pulse dialing was designed to actually move relays by the number of digits dialed (in SxS offices).

Each key on a DTMF keypad produces 2 frequencies simultaneously (one from the high group and another from the low group).

|           |   |                     |   |       |   |       |   |       |   |
|-----------|---|---------------------|---|-------|---|-------|---|-------|---|
| -----     |   |                     |   |       |   |       |   |       |   |
| Low Group | ! | Q                   | ! | ABC   | ! | DEF   | ! |       | ! |
| 697 Hz-   | ! | 1                   | ! | 2     | ! | 3     | ! | A     | ! |
|           | ! |                     | ! |       | ! |       | ! |       | ! |
|           | ! | -----               | ! | ----- | ! | ----- | ! | ----- | ! |
|           | ! | GHI                 | ! | JKL   | ! | MNO   | ! |       | ! |
| 770 Hz-   | ! | 4                   | ! | 5     | ! | 6     | ! | B     | ! |
|           | ! |                     | ! |       | ! |       | ! |       | ! |
|           | ! | -----               | ! | ----- | ! | ----- | ! | ----- | ! |
|           | ! | PRS                 | ! | TUV   | ! | WXY   | ! |       | ! |
| 852 Hz-   | ! | 7                   | ! | 8     | ! | 9     | ! | C     | ! |
|           | ! |                     | ! |       | ! |       | ! |       | ! |
|           | ! | -----               | ! | ----- | ! | ----- | ! | ----- | ! |
|           | ! |                     | ! | OPER  | ! |       | ! |       | ! |
| 941 Hz-   | ! | *                   | ! | 0     | ! | #     | ! | D     | ! |
|           | ! |                     | ! | Z     | ! |       | ! |       | ! |
|           | ! | -----               | ! | ----- | ! | ----- | ! | ----- | ! |
|           |   | 1209                |   | 1336  |   | 1477  |   | 1633  |   |
|           |   | (High Group--in Hz) |   |       |   |       |   |       |   |

A portable DTMF keypad is known as a white box.

#### TELCOM5.TXT

The fourth column (1633 Hz) is not normally found on regular fones but it does have several special uses. For one, it is used to designate the priority of calls on AUTOVON, the military fone network. These keys are called: Flash, Immediate, Priority, & Routine (with variations) instead of ABCD. Secondly, these keys are used for testing purposes by the Telco. In some areas you can find loops as well as other neat tests (see Part II) on the 555-1212 directory assistance exchange. For this, you would call up an DA in certain areas [that have an Automatic Call Distributor (ACD)] and hold down the "D" key which should blow the operator off. You will then hear a pulsing dial tone which indicates that you are in the ACD internal testing mode. You can get on one side of a loop by dialing a 6. The other side is 7. Some phreaks claim that if the person on side 6 hangs up, occasionally the equipment will screw up and start directing directory assistance calls to the other side of the loop. Another alleged test is called REMOB which allows you to tap into lines by entering a special code followed by the 7 digit number you want to monitor. Then there is the possibility of mass conferencing.

ACD's are becoming rare though. You will probably have to make several NPA-555-1212 calls before you find one.

You can modify regular fones quite readily so that they have a switch to change between the 3rd and 4th columns. This is called a silver box (aka grey box) and plans can be found in Tap as well as on many BBS's.

#### Transmitter/Receiver:

-----

When you talk into the transmitter, the sound waves from your voice cause a diaphragm to vibrate and press against the carbon granules (or another similar substance). This causes the carbon granules to compress and contract thus changing the resistance of the DC coupled path through it. Therefore, your AC voice signal is superimposed over the DC current of the local loop. The receiver works in a similar fashion where the simple types utilize a magnet, armature, & diaphragm.

#### Hybrid/Induction Coil:

-----

As you may have noticed, there are two wires for the receiver and two for the transmitter in the fone, yet the local loop consists of 2 wires instead of 4. This 4-wire to 2-wire conversion is done inside the fone by a device known as an induction coil which uses coupling transformers. All of the internal Telco trunks also use 4 wires. It is only the local loop that uses 2 since it is cheaper. A device in the CO known as a hybrid converts between 4 and 2 wire set-ups similar to the induction coil inside the fone. Special data transmission lines require extremely low signal to noise ratios, they require the full four wires--two for transmission and two for receiving (even on the local loop).

# TELCOM5.TXT

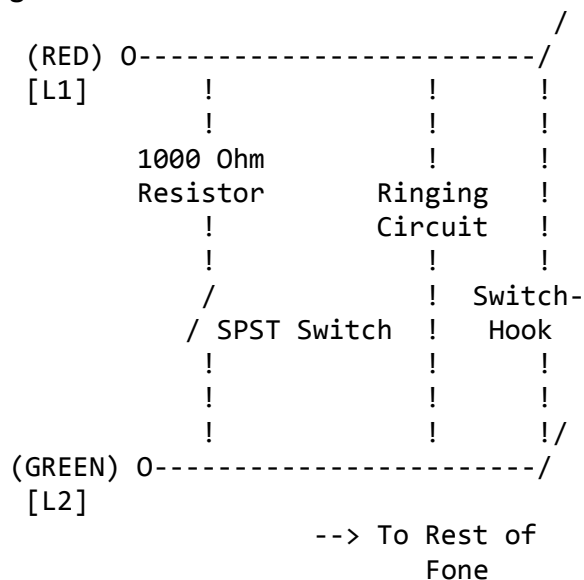
## Miscellaneous:

-----

In the telephone, there is also a balancing network consisting of a few capacitors & resistors which provide sidetone. Sidetone allows the caller to hear his own volume in the receiver. He can then adjust his voice accordingly. This prevents people from shouting or speaking too softly without noticing it.

## Hold:

When a telephone goes off hook, the resistance drops below 2500 ohms. At this point, the Telco will send a dial tone. To put someone on hold you must put a 1000 ohm resistor (1 watt) across the Tip & Ring before it reaches the switchhook. In this way, when the fone is hung up (for hold) the resistance remains below 2500 ohms which causes the CO to believe that you are still off-hook. You can build a simple hold device using the following pictorial diagram:



This hold device is only effective if you also hang up the fone. To make a hold/mute switch, simple connect a wire in place of the 1K resistor to effect a short circuit (who cares if you damage CO equipment?).

## Conclusion:

-----

NOTE: Many of the electronics components of normal fones (K500) are enclosed in the network box (which shouldn't be opened).

TELCOM5.TXT

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]?

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