Exploding The Phone

www.explodingthephone.com

Bibliographic Cover Sheet

db318

Title	**Inside Ma Bell**
Publication	*73 Magazine*
Date	1975-06-00
Author(s)	Whipple Jr., Spenser
V/I/P	p. 67
Abstract	Overview article on the operation of the telephone network from a ham radio perspective. Includes schematic circuit diagrams for red and blue boxes.
Keywords	73 Magazine; blue box; red box
Source	Alan Rubinstein

Basic Telephone Systems
Conclusion

Spenser Whipple, Jr.
c/o 73 Magazine
Peterborough NH 03458

Inside Ma Bell

The automatic couplers we have described so far would be ideal for a repeater autopatch or possibly an answering machine or automatic dialer (although we'll mention others specifically designed for answering machines and dialers later), but to connect just a few extension phones we need a bit more. We need a battery to provide power for the carbon mike, a series relay to detect when the extension goes off hook and when it dials, and also a 20 Hz ringing generator to ring bells.

While it is no great problem to build just this, if all you want is a telephone-company-approved way to connect 10 extensions in your 25-room mansion, you can order the STC Voice Connecting Arrangement for $5.80 a month plus $25 installation.

As shown in Fig. 12, the STC has only one varistor but two transformers. As usual, the main PC board (KS-20721) is used in almost a dozen different couplers and has a number of jumpers which can be hooked up in many combinations.

On the right-hand side we see that a +21 volt supply is connected to the CT output through one transformer winding, while ground is connected to the CR lead through a resistor and another transformer winding. This provides the talking power to the extension phone, and the voltage drop produced across the resistor when the extension is off hook is sensed by the control circuits and used to operate the line relay. When you pick up the extension phone, the line relay closes and puts the coupler on the line. As you dial, pulses are repeated by the line relay.

The ringing circuit is also interesting. As usual, a ring detector across the line detects the 20 Hz ringing and pulses a relay. But usually the relay pulses at 40 Hz, once on each half cycle of the 20 Hz. In this case the circuit is set up so the ring relay pulses at only 20 Hz. The ringing generator is simply a dc-to-dc inverter which changes 21 volts dc into about 120 volts dc. The ring relay contacts then change this into 20 Hz ac by

reversing the polarity at a 20 Hz rate (remember, an x means a normally open contact, while the short line means a normally closed contact). The resulting ringing signal is then applied to the CT and RV1 leads.

As mentioned in the figure caption, any number of extensions can be hooked up, but the ringing generator can only feed a maximum of three bells. This means that all the non-ringing extensions need only two-wire connections via the CT and CR leads; unfortunately the three ringing phones require a three-wire connection. This is done in order to keep the coupler simple, as it is a bit messy to test for dc continuity (off hook) on the tip and ring leads at the same time (there is 100V ac there) as it is normally done at the CO.

For some reason this coupler has the ring (CR) and tip (CT) leads mixed up. In Fig. 12, we see that the ringing generator applies its voltage between the CT (tip) lead and RV1. Since the ringer goes between the red and yellow wires in the extension (see Fig. 2), that means that the red wire has to go to the tip and the green to the ring side of the line. A rotary dial phone won't mind this, but a Touchtone phone won't work like this. You have to move the black ringer wire from the L2 terminal to the L1, and then connect red to ring (R to R) and green to tip, as normal.

Let's just quickly cover some other couplers you might be interested in:

The GC2 is just a plain ring detector, similar to the one in Fig. 7, which closes a relay contact when there is ringing voltage on your line.

The CTD is a toll-denial relay which senses long distance calls.

The C1V and HZM couplers monitor a line and provide a signal when the line is busy. Intended to allow customers to run timers or pen recorders to measure line usage.

The CEZ and CEZAW couplers allow you to make conference calls if you have two or more lines. Actually, just shorting the two lines together (tip-to-tip, ring-to-ring) would work just as well.

The CEK coupler, along with an extra line and some changes in the CO, allows you to have a message unit counter on your premises to keep track of your own message units. Probably intended for hotels and motels, which charge guests by the call.

The RDL, RDM, RDMZR, RDMZY and RDY couplers are various versions designed for telephone answering machines or for automatic recording (dictating) machines. Depending on the model, you get one-way or two-way transmission, volume limiting, or automatic cutoff when the message stops.

The RCT and RCW are couplers for recording a two-way conversation. The RCT automatically generates a beep every 15 seconds, and the RCW doesn't. I think only law enforcement agencies can get the RCW. The RCT runs $2.46 a month and $12.30 installation, while the RCW is only $1.23 a month and $12.30 installation. The RCZ is similar.

The RTT and RC1 are similar, but only beep. Used with a customer owned call duration timer, they beep to tell you you've been talking too long. The RTT sends the beep to both parties, while the RC1 only beeps the local party.

The SU7 and SU7QW (at $3.85 a month and $25 installation) allow outward dialing only for automatic dialers.

Finally, there is a group of couplers designed for burglar and fire alarm systems. Real fancy alarm systems may have a private line running straight to a police station or private detective agency; a somewhat cheaper alternative is to get an automatic dialer which dials a number and then feeds in a tape-recorded message. That's where these couplers come in (although burglar alarm installers often connect a dialer directly without a coupler.)

The CAU coupler ($4.36 a month and $14.47 installation) allows an alarm dialer to seize the line (and at the same time disconnects any other telephones on the line to prevent a burglar from interfering with the call), dial a call, and then play a pre-recorded message. It provides only one way outgoing audio transmission. An SU6AQ coupler (at $4.25 a month and $25 installation) is also for alarm systems but allows two-way voice and tone transmission; it has a ring detector and is actually built just like the STC coupler (Fig. 12) but without a ringing

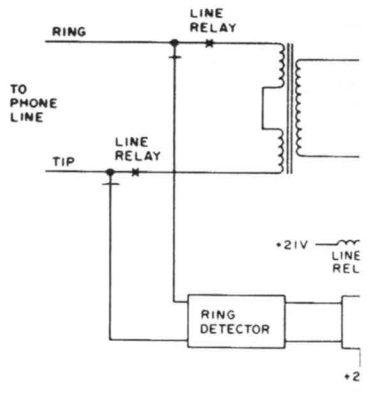


Fig. 12. Simplified diagram of ST number of extension telephones car

generator so it could be used for but not to ring them. The STS $25 installation) is the same as but with an added volume received audio.

Of greater interest, especially (though expensive compared to a version) control of things like r the SU4 or SU6 coupler. Both ar the CAU with the SU4 being o the SU6 being two way. In nc service, both of these allow an al out and send a voice or tone mess addition, they allow remote tes alarm.

They work like this: To test you need either a 1475 Hz tone g a Touchtone phone (which can high-group tone of 1477 Hz if taneously push two buttons in hand column (3-6-9). You call SU6 coupler from the outside. T detects the 20 Hz ringing, answe and automatically sends a pulse tone back to you. Now it wait 1475 Hz tone; if no such tone simply waits 20 seconds and han gets 1475 Hz, it gives the alarm have-you) a relay contact cl changes the pulsed 2125 Hz to a tone to confirm receipt. By relay closures the alarm can now 2125 Hz, send out audio (and i receive audio), or wait for furth signals. Altogether a very interest

It is fairly hard to get infor

essage unit counter on your
ep track of your own message
ly intended for hotels and
charge guests by the call.
RDM, RDMZR, RDMZY and
are various versions designed
answering machines or for
ording (dictating) machines.
the model, you get one-way
nsmission, volume limiting, or
ff when the message stops.
and RCW are couplers for
o-way conversation. The RCT
generates a beep every 15
ie RCW doesn't. I think only
nt agencies can get the RCW.
$2.46 a month and $12.30
ile the RCW is only $1.23 a
2.30 installation. The RCZ is

id RC1 are similar, but only
ith a customer owned call
they beep to tell you you've
o long. The RTT sends the
parties, while the RC1 only
arty.

d SU7QW (at $3.85 a month
ation) allow outward dialing
tic dialers.

re is a group of couplers
rglar and fire alarm systems.
n systems may have a private
aight to a police station or
ive agency; a somewhat
tive is to get an automatic
ls a number and then feeds
ded message. That's where
come in (although burglar
often connect a dialer
a coupler.)

upler ($4.36 a month and
on) allows an alarm dialer to
nd at the same time discon-
telephones on the line to
r from interfering with the
nd then play a pre-recorded
ides only one way outgoing
n. An SU6AQ coupler (at
and $25 installation) is also
s but allows two-way voice
ission; it has a ring detector
built just like the STC
2) but without a ringing

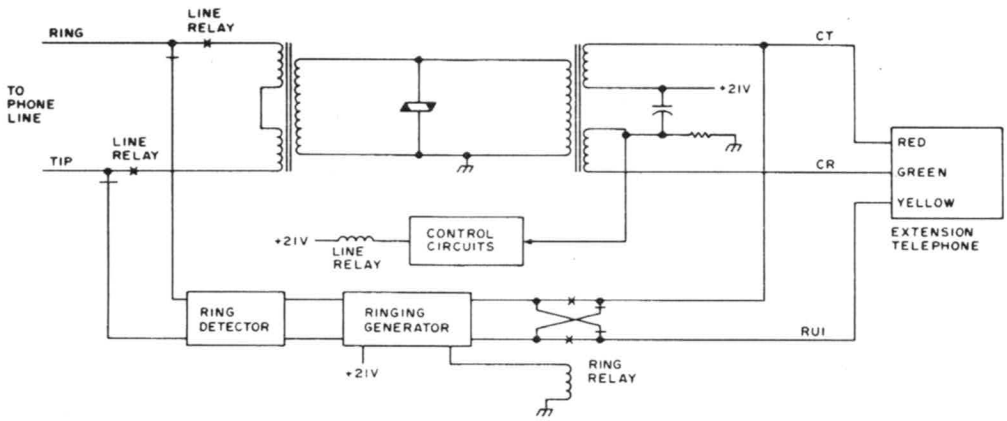


Fig. 12. Simplified diagram of STC Coupler, when equipped with options W, Z, S, P and X. Any number of extension telephones can be connected, but the ringing generator can only drive three bells.

generator so it could be used for extensions but not to ring them. The STS ($5.65 and $25 installation) is the same as the SU6AQ but with an added volume limiter for received audio.

Of greater interest, especially for simple (though expensive compared to a homebrew version) control of things like repeaters, is the SU4 or SU6 coupler. Both are similar to the CAU with the SU4 being one way and the SU6 being two way. In normal alarm service, both of these allow an alarm to dial out and send a voice or tone message. But, in addition, they allow remote testing of the alarm.

They work like this: To test the alarm, you need either a 1475 Hz tone generator or a Touchtone phone (which can generate a high-group tone of 1477 Hz if you simultaneously push two buttons in the right-hand column (3-6-9). You call the SU4 or SU6 coupler from the outside. The coupler detects the 20 Hz ringing, answers the call, and automatically sends a pulsed 2125 Hz tone back to you. Now it waits for your 1475 Hz tone; if no such tone comes, it simply waits 20 seconds and hangs up. If it gets 1475 Hz, it gives the alarm (or what-have-you) a relay contact closure, and changes the pulsed 2125 Hz to a continuous tone to confirm receipt. By appropriate relay closures the alarm can now silence the 2125 Hz, send out audio (and in the SU6, receive audio), or wait for further 1475 Hz signals. Altogether a very interesting gadget.

It is fairly hard to get information on these and other couplers from your local telephone company. For each coupler there is a Technical Reference supposedly available from "the local Telephone Company Business Office or the Marketing Representative." Unfortunately, the gals in the Business Office don't know what you're talking about, and the marketing reps have unlisted numbers. If you don't ask for too many at a time, I've found that the best way to get Technical References is with a neat letter (preferably on letterhead) to the Engineering Director, Transmission Services, American Telephone and Telegraph Co., 195 Broadway, New York, New York 10007. Publication Pub-40000 is an index of the Technical References available and is a good starting point. These publications are intended for customers and so they will tell you what the coupler will do and how to use it the way they want it used, but not what's in it. The latter information (on couplers and most other telephone company equipment and procedures) is contained in BSPs (Bell System Practices). These are "cookbooks" for installers and repairmen which tell them anything they need to know; I wouldn't be surprised if there is a BSP somewhere telling them how to climb a ladder or drive a truck.

If you've been reading carefully so far, you've probably been wondering who these phone phreaks are whom I mentioned a few thousand words ago. We've actually alluded to two other related items, the magic signalling frequency of 2600 Hz, and billing for very short calls. Maybe now is a good time

to explain. But first a word of caution: The following technical information is a matter of public knowledge and has been previously published in many places (see, for example, Esquire for October 1971 and Ramparts for June 1972 and October 1972.) Although you are free to read it and marvel at the perseverance of a group of blind kids *don't try to use it yourself.* The phone companies are very uptight about the following subjects and don't hesitate to prosecute anyone they catch using the techniques we're about to describe.

Sometime in the late sixties, a few blind kids interested in the phone company happened to meet at a camp for the blind. By pooling their knowledge and talents (excellent hearing and musical pitch, as well as lots of free time to experiment) they were able to develop a number of techniques for placing and receiving free long distance calls. Elated with their knowledge, they got great kicks out of routing their calls through foreign countries and even all around the world. Some of them even got to be quite famous — ever hear of Captain Crunch and his magic whistle, which just happened to whistle at 2600 Hz?

The simplest of their techniques involves the so-called black box, which allows you to receive free long-distance calls (calls for which the other party is not charged). It works like this:

When someone calls your number, the dial system connects his phone to your phone and then starts ringing your bell. If you had a way of coupling to your line *between the rings* in such a way that you didn't complete the dc circuit, you could actually talk to him without his being charged for the call, because as far as the CO is concerned, there is no dc connection and therefore there is no answer at your end.

Of course, the 90 volt ringing signal makes it tricky, because it can blow your eardrum out. Wouldn't it be nice if you could stop it? Then you could talk continuously. But we mentioned earlier that the call doesn't register unless it lasts a second or so. By picking up and then slamming down the regular telephone set as fast as possible (or having a ring-detector relay as in Fig. 7 with its n.o. contacts right across the line, which puts a very fast short circuit across the line), you get the bell to stop! That's all there is to the Black Box.

Somewhere along the line, somebody came up with an even neater version: if a 10k resistor is placed in series with the phone, enough dc current passes through to provide talk current for the carbon mike, but not enough to trip the CO relays. A 1μF capacitor or so across the resistor is needed to let audio through, as well as an SPST switch to remove the resistor when not needed. On a 500 style telephone the extra capacitor is not even needed if the 10k resistor is placed between the F and RR terminal on the network (see Fig. 3) and the switch is placed in series with the pulsing contacts of the dial.

Before continuing, let us again stress the admonition that you not use any of these ideas — they are presented here only for your own information. As mentioned earlier, widespread usage of any of these techniques could cause havoc and the telephone companies are determined to catch any users as fast as possible. They are hard at work to develop equipment which would identify and trace such calls, and a number of people have already been prosecuted. For example, rumor has it that black boxes can be detected on calls longer than a minute or two in duration.

Another device is popularly called the Red Box. If you remember the old-style coin phones with three coin slots on top (nickel, dime, and quarter), you may remember the sounds they made when you dropped a coin in — two bells inside made a ding on a nickel, a ding-ding on a dime, and a bong on a quarter. Unfortunately, some unscrupulous individuals either looted a pay-phone and stole the bells, or tape-recorded the sound, and then used this to fool operators into thinking that calls were being paid for. To counter this, a new coin phone was designed which used an electronic oscillator, rather than a bell, to signal the type of coin inserted. When the oscillator is on, the earphone is muted so you can't hear it, and an electronic gizmo indicates to the operator how much money was inserted.

The Red Box is simply a 2.2 kHz oscillator, switched on and off electronically just

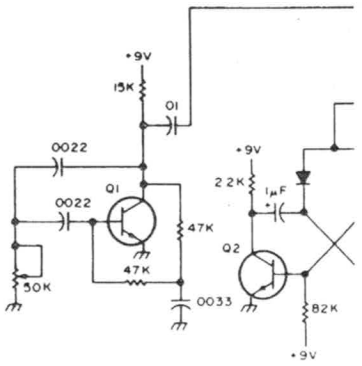


Fig. 13. Early version of the Red B diodes 1N914 or similar, resistors polystyrene.

like the one in the payphone, w speaker to couple it to the mike. are coded as follows:

Nickel — One 60 millisecond puls

Dime — Two 60 ms pulses separ ms;

Quarter — Five 35 ms pulses sepa ms.

Some of the phone phreaks mu knowledgeable about electronics Box circuits are reasonably mod using ICs.

Fig. 13 shows an early version Box. To see how it works, supp button is pushed. This starts multivibrator (Q2 and Q3), whic turning it on 60 ms, and off shorts the output of Q1, th oscillator, generating pulses of tc Q7 are a timer that lets exactly t pulses reach the IC, which feed True to form, the phone phreal use a 600 Ohm earpiece (borro phone handset) rather than speaker.

A later version, in Fig. 14, is more sophisticated. IC1 is the t IC2 is the astable.

The most famous (and most well as most dangerous) is the Because it goes to the heart of l

ery fast short circuit across
et the bell to stop! That's all
lack Box.

along the line, somebody
an even neater version: if a
placed in series with the
dc current passes through to
rrent for the carbon mike,
ı to trip the CO relays. A
or so across the resistor is
udio through, as well as an
emove the resistor when not
00 style telephone the extra
t even needed if the 10k
d between the F and RR
network (see Fig. 3) and the
in series with the pulsing
ial.

uing, let us again stress the
you not use any of these
e presented here only for
ation. As mentioned earlier,
of any of these techniques
avoc and the telephone
termined to catch any users
e. They are hard at work to
ent which would identify
alls, and a number of people
n prosecuted. For example,
hat black boxes can be
s longer than a minute or

ce is popularly called the
remember the old-style coin
e coin slots on top (nickel,
r), you may remember the
e when you dropped a coin
inside made a ding on a
g on a dime, and a bong on
unately, some unscrupulous
looted a pay-phone and
r tape-recorded the sound,
his to fool operators into
ls were being paid for. To
ew coin phone was designed
lectronic oscillator, rather
signal the type of coin
the oscillator is on, the
d so you can't hear it, and
no indicates to the operator
was inserted.
is simply a 2.2 kHz oscill-
and off electronically just

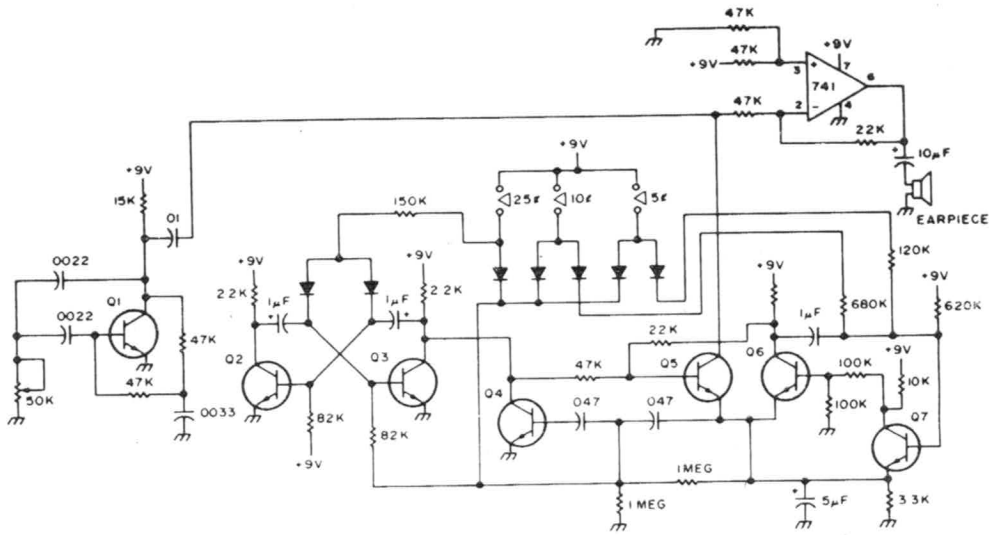


Fig. 13. Early version of the Red Box, circa 1972. Transistors are NPN silicon (2N2222 or HEP55), diodes 1N914 or similar, resistors ¼ Watt, 5%. Small capacitors are high quality mylar, epoxy, or polystyrene.

like the one in the payphone, with a small speaker to couple it to the mike. The pulses are coded as follows:

Nickel – One 60 millisecond pulse;

Dime – Two 60 ms pulses separated by 60 ms;

Quarter – Five 35 ms pulses separated by 35 ms.

Some of the phone phreaks must be fairly knowledgeable about electronics as the Red Box circuits are reasonably modern – even using ICs.

Fig. 13 shows an early version of the Red Box. To see how it works, suppose the 10¢ button is pushed. This starts an astable multivibrator (Q2 and Q3), which feeds Q5, turning it on 60 ms, and off 60 ms. Q5 shorts the output of Q1, the 2.2 kHz oscillator, generating pulses of tone. Q6 and Q7 are a timer that lets exactly two of these pulses reach the IC, which feeds a speaker. True to form, the phone phreaks prefer to use a 600 Ohm earpiece (borrowed from a phone handset) rather than buying a speaker.

A later version, in Fig. 14, is quite a bit more sophisticated. IC1 is the timer, while IC2 is the astable.

The most famous (and most powerful as well as most dangerous) is the Blue Box. Because it goes to the heart of long distance switching systems, let's talk about long distance calls for a while.

All the way at the beginning of this article, in Fig. 1, we showed your local CO as being connected to other local subscribers, other COs, and also to long distance switching centers; the latter are called "tandems."

There are many COs in any city, just as there are many tandems throughout the country. It would clearly be impractical for every CO to be connected directly to every other CO, and likewise it's not practical for every tandem to be connected directly to every other tandem. This means that in a few instances (such as over common routes – say, New York to Chicago) a long distance call may be routed directly from a tandem near New York to another tandem near Chicago. But many times a call may have to be routed through several tandems – Chicago to San Diego, for instance, might go through Los Angeles. Because of this, the tandems are so arranged that if they cannot route a call directly (either because all direct lines are busy, or else there are no direct lines) they simply route a call some more indirect way. Also, if a tandem office receives a call not intended for it, it just relays it on in the right direction.

Whenever there is a direct connection

between tandem offices, that may consist of many lines, carrying many simultaneous conversations. Actually, we shouldn't use the word "lines," because in reality these conversations may be multiplexed onto coaxial cables or microwave links. This means that dialing can't take the form of dc pulses, as in your home phone, but always consists of pairs of tones called multi-frequency or MF tones, similar to Touch-tone dialing. The only difference is that the frequencies are different from those used in Touchtone dialing, as follows:

Digit	Frequencies (Hz)
1	700 + 900
2	700 + 1100
3	900 + 1100
4	700 + 1300
5	900 + 1300
6	1100 + 1300
7	700 + 1500
8	900 + 1500
9	1100 + 1500
0	1300 + 1500

In addition, 3 additional signals are:

KP (Key Pulses)	1100 + 1700
ST (start)	1500 + 1700
Disconnect	2600

Another aspect to keep in mind is that it takes quite a bit of equipment to establish a connection, but little equipment is needed to maintain it. To avoid useless duplication, the equipment used to set up a connection (called a sender) is shared among many lines. Whenever a sender has a call to handle, it searches for an idle line; when it finds one it latches onto it and then forwards the call. As soon as it is finished, the sender leaves the call and goes to service another call. To mark an idle line, the tandem office feeds a 2600 Hz tone into it.

Now let's examine a typical call – suppose you place a call from New York to Los Angeles. You pick up your phone in New York and dial area code 213 for Los Angeles, followed by the seven-digit number. That number is stored in a register in your CO, and now two things happen. First, an accounting machine called CAMA – Centralized Automatic Message Accounting – keeps track of your call. This is done by punching your number, the time, and the number you dialed into a paper tape (which will later be fed to a computer). Your CO now sets up a connection with the nearest tandem office and sends the area code and number you dialed to the tandem. In the tandem a sender decides on the route, and starts looking for an idle line. Suppose there is an idle direct connection from this tandem to the one in L.A. Since this line can be used for calls in either direction, both tandems are marking it as idle by feeding 2600 Hz

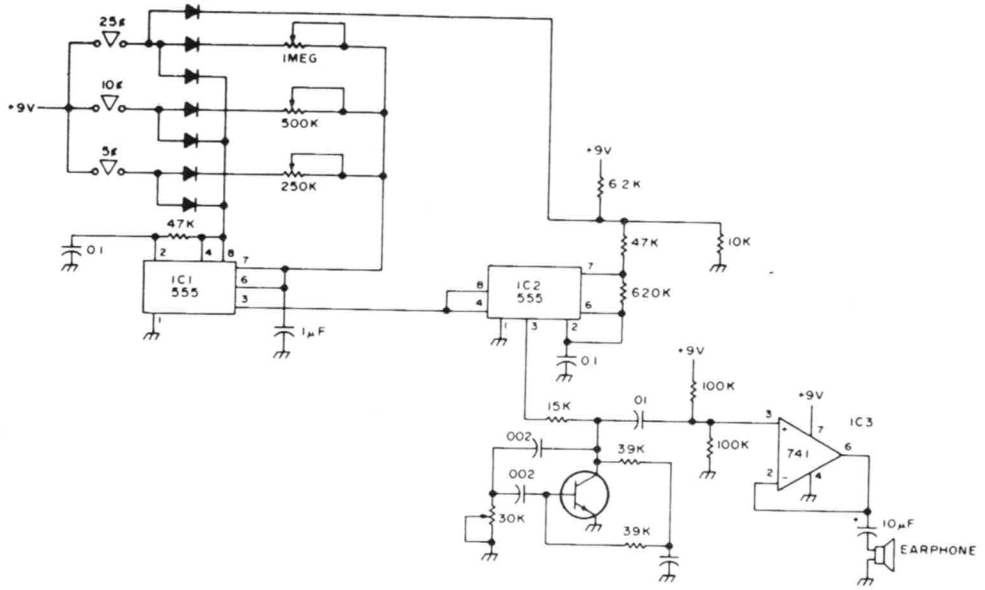
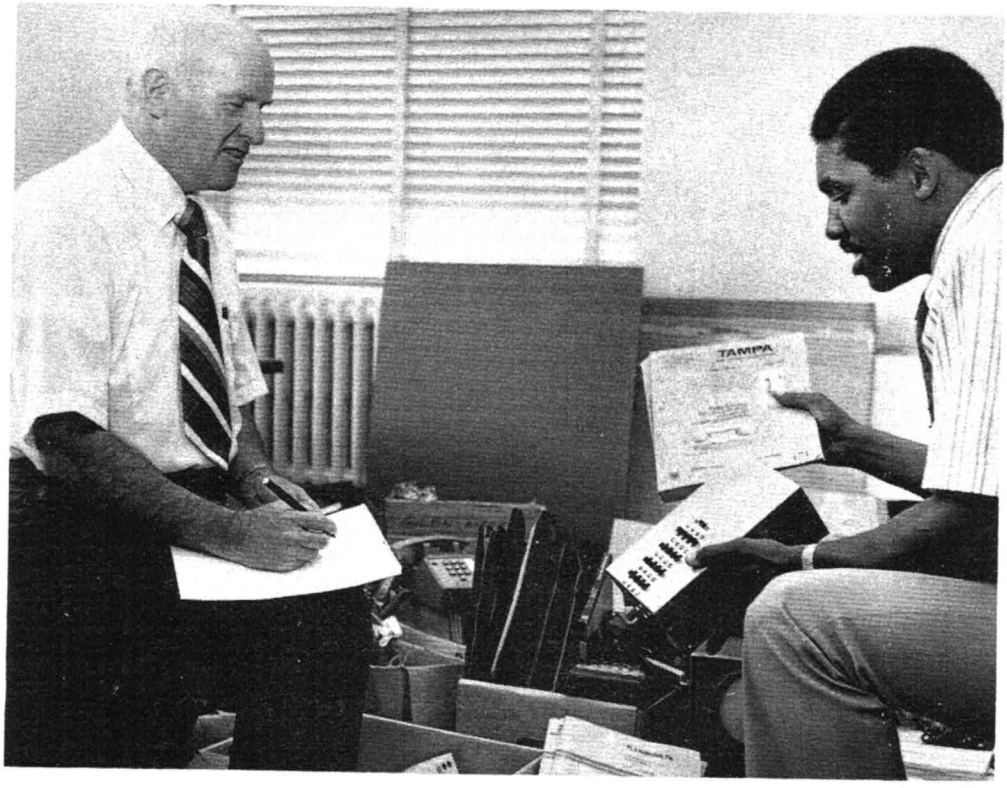


Fig. 14. Later version of the Red Box, circa 1973.



Chester County (Pa.) Detective Ronald Johnson (right) displays an illegal "Blue Box" used to bypass toll charges and seize long distance telephone circuits. Johnson and Chief of County Detectives Eugene Sharpe (left) were part of a law enforcement team which raided several Chester County residences of suspected "phone phreaks." Four persons were arrested in connection with charges ranging from toll fraud to impersonation of telephone company employees and, in one case, wiretapping. Authorities said "several carloads" of illegal equipment were confiscated, some of which is shown here.

into it, one from each end.

Now the sender finds this idle line. First, to prevent L.A. from trying to send a call in the opposite direction at the same time, the New York sender removes its 2600 Hz tone. This tells L.A. that a call is about to come on this line, and so L A. assigns an incoming sender to it. The New York sender sends the 213 area code and the 7-digit number to L.A., using the MF (multi-frequency) tones described earlier. The code is preceded by the KP tones, and followed by the ST tones. The LA tandem office decodes the tones and, in this case, connects you to the CO serving the party you dialed. The CO now decodes the last four digits of the number, connects you to the proper line, and starts ringing it.

When the other party answers, the ringing stops and a signal is sent all the way back to your CO to indicate that the call has reached its destination. This too is punched into the CAMA paper tape.

If you hang up first, your CO of course knows this immediately. On the other hand, if the party hangs up first, a signal has to be sent back to your CO. The L.A. CO notifies the L.A. tandem, the L.A. tandem puts 2600 Hz back on the line to signify a disconnect, the New York tandem gets the tone and breaks the connection, and notifies your CO. If you listen carefully, you may hear a short burst of 2600 Hz just before the connection is broken at your end.

At this point your CO again punches your number, the time and the number you dialed

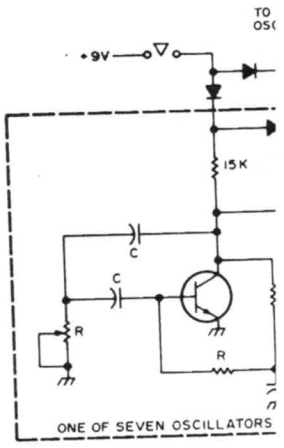


Fig. 15. Early version

into paper tape. Once a da
to the computer, which th
and eventually uses it to pre

The CAMA tape runs o
calls on which there is no
are free (such as informati
area code 800). It's up to
decide at the end of the m
and how much. This, by th
to detect black, blue and
record is kept of all calls
can be programmed to
picious calls.

Now, where does the
the story? The Blue Box
thirteen buttons and t
generate the MF tones –
ST and 2600 Hz disconne
acoustically coupled from
the mike of the phone.
phreak can use the toll ci
anywhere in the world wi
enough knowledge of th
route himself via a spec
even choose whether he
satellite. Some phone
sitting in a phone booth a
the very next booth all t
whole globe; then they
and enjoy the fact that th
by having to travel all t
world.

The procedure for us
simple. You start by pla
call in the normal wa
number (information o

"Blue Box"
on and Chief
team which
our persons
sonation of
aid "several

s, the ringing
way back to
I has reached
ched into the

CO of course
e other hand,
nal has to be
. CO notifies
m puts 2600
disconnect,
ne tone and
ies your CO.
hear a short
e connection

unches your
r you dialed

3 MAGAZINE

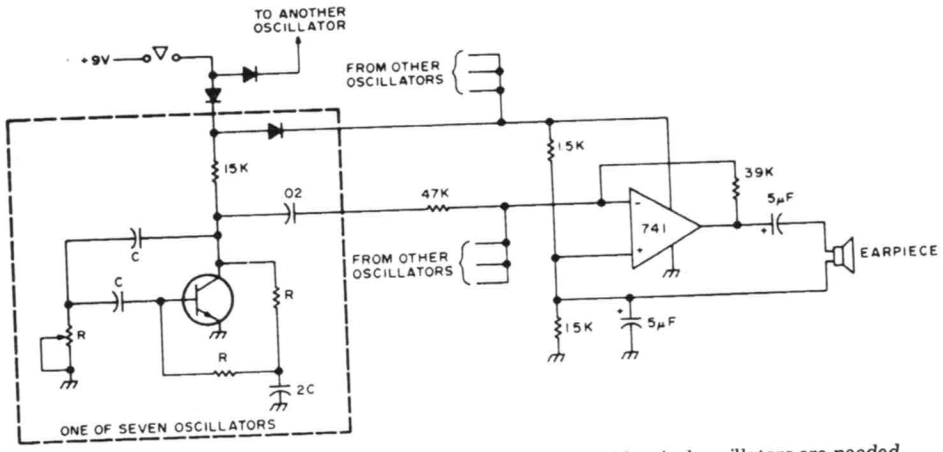


Fig. 15. Early version of the Blue Box, circa 1972. Seven identical oscillators are needed.

into paper tape. Once a day this tape is sent to the computer, which then reads the tape and eventually uses it to prepare the bill.

The CAMA tape runs on every call, even calls on which there is no answer, or which are free (such as information calls or calls to area code 800). It's up to the computer to decide at the end of the month what to bill and how much. This, by the way, is one way to detect black, blue and red boxes since a record is kept of all calls and the computer can be programmed to look for any suspicious calls.

Now, where does the Blue Box fit into the story? The Blue Box is just a box with thirteen buttons and the oscillators to generate the MF tones – 0 through 9, KP, ST and 2600 Hz disconnect. These tones are acoustically coupled from the Blue Box into the mike of the phone. With it the phone phreak can use the toll circuits to place calls anywhere in the world without charge. With enough knowledge of the system he can route himself via a specific path and can even choose whether he will go via cable or satellite. Some phone phreaks delight in sitting in a phone booth and routing a call to the very next booth all the way around the whole globe; then they talk to themselves and enjoy the fact that their voice is delayed by having to travel all the way around the world.

The procedure for using the Blue Box is simple. You start by placing a long distance call in the normal way either to a free number (information or a valid 800 series number) or else to a close-by destination which is cheap to call. This is the call which will appear on the CAMA tape. Since a long call to information or to a non-existent number is suspicious, dedicated phone phreaks usually make sure to use a valid 800 number or, if not too stingy (or stubborn), even a paid call to a nearby place.

Once dialing is completed, your nearby tandem routes the call to the tandem office at the destination, possibly through intermediate tandems along the way. As soon as you hear ringing from the other end, you feed 2600 Hz into your phone for one second.

Your local CO is unaccustomed to getting 2600 Hz and so simply ignores it, but passes it on to the nearby tandem.

This tandem can recognize 2600 Hz as a disconnect idle from other tandems, but is not built to react to the signal coming from a CO. So it ignores it and passes it on. But the *next* tandem, thinking you hung up, cancels the call. This leaves you hanging, still connected to a toll line between tandems. After one second of 2600 Hz, you remove it. The distant tandem now sees that the line is no longer idle, and so it connects an incoming sender. As soon as you hear the click signifying this, you have ten seconds to dial the desired number, preceded by KP and followed by ST. For example, to call (603) 924-3873 you would press KP6039243873ST.

When the number answers, a signal is sent back and the CAMA tape punched to indi-

cate the connection time. At the end of the call, the CAMA tape is again punched with your number, the time and the number you originally dialed. This is the call and time for which you will be billed (unless it is free) and the number actually reached with the Blue Box is not recorded.

Since all calls are punched into the CAMA tape, even the most daring phone phreakers would use a pay phone rather than their home phone. Moreover, since the mere possession of a Blue Box might be considered suspicious, some record the tones on a cassette and then erase it as soon as possible. The actual Blue Box circuitry is interesting not only for the insight into the technical competence of the phone phreaks, but also because with just a retuning, it can be used for Touchtone generation.

Fig. 15 shows an early version of a Blue Box, where each tone is generated by a separate one-transistor oscillator. There would be a total of 7 oscillators and 13 push-buttons, with each push-button (except the 2600 Hz disconnect/idle button) feeding two oscillators, through a diode.

The Twin-Tee oscillators generate a relatively clean sine wave, but some juggling of values is needed. The oscillation frequency is

$$f = \frac{1}{2\pi RC}$$

where the best values for R are between about 30k and 100k. In all of these circuits, see Fig. 15 for component data. Since disk capacitors are very unstable with temperature, frequency-determining capacitors should be good quality mylar or preferably polystyrene.

Fig. 16 shows a later version of the Blue Box, showing real state-of-the-art design with all ICs. The LM100 (or LM300) regulator is needed to assure stable frequency characteristics — my own preference is a 723, which uses a similar circuit, and is easier to get.

The use of the Intersil 8038CC shows a good knowledge of the field by whoever designed this circuit in late '73 or early '74. The uninitiated wouldn't know about this new ultra-stable IC which, unlike the 566 or other popular oscillator ICs, generates a very low-distortion sine wave. Only two oscillators are needed, as the switches and diodes select different pots for different tones. Although most Blue Boxes seem to use plain push-buttons, Chomerics makes nice switches which are suitable.

Just to give you an idea of the power of the Blue Box, here are some numbers and destinations that have been published in various places:

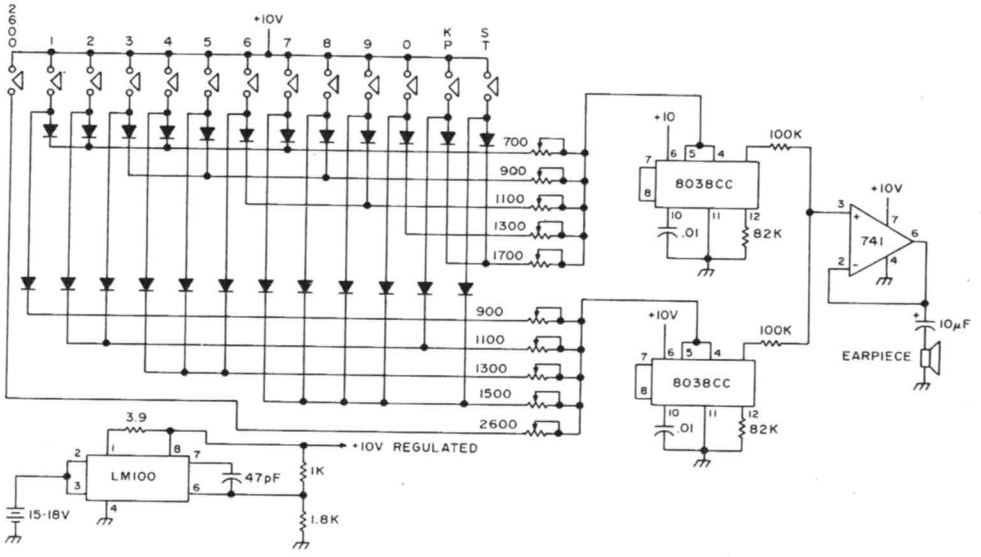


Fig. 16. Later version of the Blue Box, circa 1974. The pots are 25k; .01 uF capacitors are mylar or polystyrene.

London weather: KP 044 1 246 8091 ST
Sidney, Australia weather: KP 061 3 6064 ST
Sidney time: KP 061 2 2074 ST

The digits 044 or 061 in the above numbers are the country codes agreed on by the CCITT; further information on country codes, Blue Box tone frequencies, etc., is published in Chapter 2 of *Reference Data for Radio Engineers* (Howard W. Sams) as well as in an underground (and sometimes nasty and violent) newsletter called TAP ($2 for a one-year subscription from TAP, Room 504, 152 West 42 Street, New York NY 10036).

Further information may be obtained from a book entitled *Basic Telephone Switching Systems* by David Talley (Hayden Book Company), *Communications System Engineering Handbook* edited by D. Hamsher (McGraw-Hill Book Company) and various telephone company periodicals. *The Bell System Technical Journal* should be available in most engineering college libraries, and carries a lot of abstract and mathematical articles as well as some fairly practical descriptions. For example, the November 1960 issue has an article on "Signaling Systems for Control of Telephone Switching." A much more readable publication is the *GTE Lenkurt Demodulator* (GTE Lenkurt, 1105 Country Road, San Carlos CA 94070) which is a monthly magazine available free to people working in the communications field or in schools.

The GTE equivalent of the Bell Systems Practices is called the General System Practices, and may just possibly be available locally or from GTE Automatic Electric Inc., Northlake, Illinois. You may also be able to get your hands on a mail-order course offered some years ago by Don Britton Enterprises in Hawaii. A new book, *How to Cut Costs and Improve Service of Your Telephone, Telex, TWX and Other Telecommunications* by Frank Griesinger (McGraw-Hill) and a monthly magazine called "Communications News" are other possible sources.

In closing, I would again like to caution readers that the telephone companies do their best to "discourage" the use of the various colored boxes described in this article; the information presented here has been written only for your own information and entertainment, not as a guide for construction or use.

(AUTHOR'S NOTE: Some time after this article was written, AT&T, in response to a complaint lodged with the FCC by Phone-Mate Corp., a large manufacturer of telephone answering machines, made a concession in its insistence on the use of a coupler with an answering machine. It applies *only* to telephone answering machines though. For a fee, the Bell System will license the answering machine manufacturer to build and install a coupler directly into the answering machine, using a design developed by Bell System engineers. The coupler consists of several transistors, resistors and capacitors, limiting diodes, a relay, and a three-winding transformer, and is estimated to cost less than $20 to build. It is basically a receive-only coupler which prevents the answering machine from dialing outgoing calls. Although further details haven't been released at the time of writing, it doesn't look as though the answering machine manufacturers will be making these couplers separately for updating older machines, and there seem to be quite a few strings attached.)

(SECOND AUTHOR'S NOTE: Gradually, more details are coming out about the strings attached to the coupler offer to answering machine manufacturers. AT&T will consider only inquiries from actual manufacturers, who must submit a $1000 non-refundable "inspection fee," for which AT&T will send a team to inspect the manufacturer's factory to determine whether he is "qualified" to manufacture the coupler. Only if he passes, will AT&T discuss the price with him, apparently on a take-it-or-leave-it basis. The coupler design appears to be more complicated than was announced originally, and includes an opto-electronic coupler – neon bulb/photocell combination – to detect ringing, similar to the circuit on page 31 of the April 1974 issue of 73 Magazine. Only time will tell how many answering machine manufacturers will decide to gamble the $1000 on such a basis.)

. . . WHIPPLE

Dirt Che for

Having a 6 meter Tunaver tried it with various sr radios, I thought there had to better. I began to look for a u auto radio that was small and lucky – I found two that w foreign cars (one was a Mot other was a Peptone, which Volkswagen uses) and they c two. One had a broken pla (which epoxy cured) and the dirty.

I saw a picture of a set-up mounted a car radio and c cabinet, making a VHF solid s he was using it as it was. Motorola to change. Be sure your radio before any chan repairs if needed. As is, they hard on batteries (even sma you have a transistor transmit lator working from the sam power stage alone, accordi records, draws 350 mA. Stil dry batteries?

I took the cheap way out. stripped AM/FM radio and I t and cut the push-pull audi repaired the broken (sawed soldered leads to it and mou radio where the original outp had been located. Mine h ground, so I had to insula chassis by fiber washers.

The emitter's resistor was but the transistors heated up so I broke the lead and add resistor and all was well. My