G-File: The Official Phreakers Manual Document - PHREAK*.DOC
Reconstructed 1990/9/11 <<> westsmith

THE OFFICIAL PHREAKERS MANUAL

jack the ripper
Ripper

Introduction

What precedes this introduction is what I have termed "The Official Phreakers Manual", while it may not be. Many times I have been on a BBS, which has files claiming to have summed up all the ways to phreak in the U.S. and abroad, well those were pretty lame and a couple pages long. Now after many relentless hours of work, I have done it. This is an informative file and the authors of this and the authors from which I have gathered information, take absolutely NO responsibility and are not liable for, under any circumstances for damage, direct, indirect, incidental, or consequential.

> Warning: Use of this material may shorten your life in the free world!

Ok enough of the bullshit, I readily admit that this is mainly a compilation of available phreak material and public resources. What I have done is to gather it all together and edit, compile, check for errors, put in a readable form, and finally to write what I know without echoing what others have said. I have set this up that it is good for all levels of phreaks, going from novice to advanced, and references and tables for easy reference in the back.

This manual is constantly being updated! If you have any contributions or corrections or comments, please leave messages to me (Jack the Ripper) on any BBS's I am on (probably where you got it). Thanks!

Table of Contents

Appendixes

Chapter 1

Ok this chapter will cover the basic vocabulary of phreaking, it is a fairly long list, though not totally complete. After the vocab, will be some of the general rules for phreaking. Most of the rules are protection from the police and AT&T, but others are grammatical rules. These are not as important to your freedom, but many a phreak will think you are a twelve year old if you start talking like, "Hey dudz!^$(&, just got the latest warez! trade u for some soft/docs. Checkul8r". Well you get the point, here's your vocab list ...

The Bell Glossary

By Mad Marvin

ACD
Automatic Call Distributor - A system that automatically distributes calls to operator pools (providing services such as intercept and directory assistance), to airline ticket agents, etc.

Administration
The tasks of record-keeping, monitoring, rearranging, prediction need for growth, etc.

AIS
Automatic Intercept System - A system employing an audio-response unit under control of a processor to automatically provide pertinent info to callers routed to intercept.

Alert
To indicate the existence of an incoming call, (ringing).

ANI
Automatic Number Identification - Often pronounced "Annie," a facility for automatically identify the number of the calling party for charging purposes.

Appearance
A connection upon a network terminal, as in "the line has two network appearances."

Attend
The operation of monitoring a line or an incoming trunk for off-hook or seizure, respectively.

Audible
The subdued "image" of ringing transmitted to the calling party during ringing; not derived from the actual ringing signal in later systems.

Backbone Route
The route made up of final-group trunks between end offices in different regional center areas.

BHC
Busy Hour Calls - The number of calls placed in the busy hour.

Blocking
The ratio of unsuccessful to total attempts to use a facility; expresses as a probability when computed a priority.

Blocking Network
A network that, under certain conditions, may be unable to form a transmission path from one end of the network to the other. In general, all networks used within the Bell Systems are of the blocking type.

Blue Box
Equipment used fraudulently to synthesize signals, gaining access to the toll network for the placement of calls without charge.

BORSCHT Circuit
A name for the line circuit in the central office. It functions as a mnemonic for the functions that must be performed by the circuit: Battery, Overvoltage, Ringing, Supervision, Coding, Hybrid, and Testing.

Busy Signal
(Called-line-busy) An audible signal which, in the Bell System, comprises 480Hz and 620Hz interrupted at 60IPM.

Bylink
A special high-speed means used in crossbar equipment for routing calls incoming from a step-by-step office. Trunks from such offices are often referred to as "bylink" trunks even when incoming to noncrossbar offices; they are more properly referred to as "DC incoming trunks." Such high-speed means are necessary to assure that the first incoming pulse is not lost.

Cable Vault
The point which phone cable enters the Central Office building.

CAMA

Centralized Automatic Message Accounting - Pronounced like Alabama.

CCIS
Common Channel Interoffice Signaling - Signaling information for trunk connections over a separate, nonspeech data link rather that over the trunks themselves.

CCITT
International Telegraph and Telephone Consultative Committee - An International committee that formulates plans and sets standards for intercountry communication means.

CDO
Community Dial Office - A small usually rural office typically served by step-by-step equipment.

CO
Central Office - Comprises a switching network and its control and support equipment. Occasionally improperly used to mean "office code."

Centrex
A service comparable in features to PBX service but implemented with some (Centrex CU) or all (Centrex CO) of the control in the central office. In the later case, each station's loop connects to the central office.

Customer Loop
The wire pair connecting a customer's station to the central office.

DDD
Direct Distance Dialing - Dialing without operator assistance over the nationwide intertoll network.

Direct Trunk Group
A trunk group that is a direct connection between a given originating and a given terminating office.

EOTT
End Office Toll Trunking - Trunking between end offices in different toll center areas.

ESB
Emergency Service Bureau - A centralized agency to which 911 "universal" emergency calls are routed.

ESS
Electronic Switching System - A generic term used to identify as a class, stored-program switching systems such as the Bell System's No.1 No.2, No.3, No.4, or No.5.

ETS
Electronic Translation Systems - An electronic replacement for the card translator in 4A Crossbar systems. Makes use of the SPC 1A Processor.

False Start
An aborted dialing attempt.

Fast Busy (often called reorder)
An audible busy signal interrupted at twice the rate of the normal busy signal; sent to the originating station to indicate that the call blocked due to busy equipment.

Final Trunk Group
The trunk group to which calls are routed when available high-usage trunks overflow; these groups generally "home" on an office next highest in the hierarchy.

Full Group
A trunk group that does not permit rerouting off-contingent foreign traffic; there are seven such offices.

Glare
The situation that occurs when a two-way trunk is seized more or less simultaneously at both ends.

High Usage Trunk Group
The appellation for a trunk group that has alternate routes via other similar groups, and ultimately via a final trunk group to a higher ranking office.

Intercept
The agency (usually an operator) to which calls are routed when made to a line recently removed from a service, or in some other category requiring explanation. Automated versions (ASI) with automatic voiceresponse units are growing in use.

Interrupt
The interruption on a phone line to disconnect and connect with another station, such as an Emergence Interrupt.

Junctor
A wire or circuit connection between networks in the same office. The functional equivalent to an intraoffice trunk.

MF
Multifrequency - The method of signaling over a trunk making use of the simultaneous application of two out of six possible frequencies.

NPA
Numbering Plan Area.

ONI
Operator Number Identification - The use of an operator in a CAMA office to verbally obtain the calling number of a call originating in an office not equipped with ANI.

PBX
Private Branch Exchange - (PABX: Private Automatic Branch Exchange) An telephone office serving a private customer, Typically , access to the outside telephone network is provided.

Permanent Signal
A sustained off-hook condition without activity (no dialing or ringing or completed connection); such a condition tends to tie up equipment, especially in earlier systems. Usually accidental, but sometimes used intentionally by customers in high-crime-rate areas to thwart off burglars.

POTS
Plain Old Telephone Service - Basic service with no extra "frills".

ROTL
Remote Office Test Line - A means for remotely testing trunks.

RTA
Remote Trunk Arrangement - An extension to the TSPS system permitting its services to be provided up to 200 miles from the TSPS site.

SF
Single Frequency. A signaling method for trunks: 2600Hz is impressed upon idle trunks.

Supervise
To monitor the status of a call.

SxS
(Step-by-Step or Strowger switch) - An electromechanical office type utilizing a gross-motion stepping switch as a combination network and distributed control.

Talkoff
The phenomenon of accidental synthesis of a machine-intelligible signal by human voice causing an unintended response. "whistling a tone".

Trunk
A path between central offices; in general 2-wire for interlocal, 4-wire for intertoll.

TSPS
Traffic Service Position System - A system that provides, under stored-program control, efficient operator assistance for toll calls. It does not switch the customer, but provides a bridge connection to the operator.

X-bar
(Crossbar) - An electromechanical office type utilizing a "fine-motion" coordinate switch and a multiplicity of central controls (called markers). There are four varieties:

No.1 Crossbar — Used in large urban office application; (1938)

No 3 Crossbar — A small system started in (1974).

No.4A/4M Crossbar — A 4-wire toll machine; (1943).

No.5 Crossbar — A machine originally intended for relatively small suburban applications; (1948)

Crossbar Tandem — A machine used for interlocal office switching.

The MCI Telecommunications Glossary
Part I Volume I (A - D)

Metal Shop: (314) 432-0756
Typed by Knight Lightning

A&B Leads
Designation of leads derived from the midpoints of the two 2-wire pairs comprising a 4-wire circuit.

Abbreviated Dialing
The ability of a telephone user to reach frequently called numbers by using less than seven digits. Synonym: Speed Dialing

Access Charge
A fee paid for the use of local lines.

Access Code
A digit or number of digits required to be connected to a private line arranged for dial access.

Access Line
A telephone circuit which connects a customer location to a network switching center.

Airline Mileage
Calculated point-to-point mileage between terminal facilities.

All Trunks Busy (ATB)
A single tone interrupted at a 120 ipm (impulses per minute) rate to indicate all lines or trunks in a routing group are busy.

Alternate Route
A secondary communications path used to reach a destination if the primary path is unavailable.

Alternate Use
The ability to switch communications facilities from one type of service to another, i.e., voice to data, etc.

Alterante Voice Data (AVD)
A single transmission facility which can be used for either voice or data.

American Standard Code for Information Interchange (ASCII)
An 8 level code developed for the interchange of information between data processing and communications systems.

Analog Signal
A signal in the form of a continuous varying physical quantity, e.g., voltage which reflects variations in some quantity, e.g., loudness in the human voice.

Annunciator
An audible intercept device that states the condition or restrictions associated with circuits or procedures.

Answer Back
An electrical and/or visual indication to the calling or sending end that the called or received station is on the line.

Answer Supervision
An off-hook signal transmitted toward the calling end of a switched connection when the called party answers.

Area Code
Synonym: Numbering Plan Area (NPA). A three digit number identifying more than 150 geographic areas of the United States and Canada which permits direct distance dialing on the telephone system. A similar global numbering plan has been established for international subscriber dialing.

Attendant Position
A telephone switchboard operator's position. It provides either automatic (cordless) or manual (plug and jack) operator controls for incoming and/or outgoing telephone calls.

Attenuation
A general term used to denote the decrease in power between that transmitted and that received due to loss through equipment, lines, or other transmission devices. It is usually expressed as a ration in db (decibel).

Audible Ringing Tone
An audible signal heard by the calling party during the ringing-interval.

Authorization Code
An identification number that the caller enters when placing a call which is used for billing purposes.

Authorized User
A person, firm, organization, corporation or any other entity authorized by the customer to send or receive communications over a specific communications network.

Auto Answer
A machine feature that allows a transmission control unit or station to automatically respond to a call that it receives.

Automatic Call Distributor
A switching system designed to queue and/or distribute a large volume of incoming calls to a group of attendants to the next available "answering" position.

Automatic Dialing Unit
A device which automatically generates a predetermined set of dialing digits.

Automatic Identification of Outward Dialing (AIOD)
A computer generated report showing all long distance calls placed over AT&T's toll network.

Automatic Number Identification (ANI)

Automatic equipment at a local dial office used on customer dialed calls to identify the calling-station.

Automatic Route Selection (ARS)
Least cost routing via AT&T CENTREX system.

Band
(1) The range of frequencies between two defined limits. (2) In reference to WATS, one of the five specific geographic areas as defined by AT&T. Synonym: BANDWIDTH.

Bandwidth
See BAND.

Baseband
The total frequency band occupied by the aggregate of all the voice and data signals used to modulate a radio carrier.

Baud
A unit of signaling speed. The speed in baud is the number of discrete conditions conditions or signal elements per second. If each signal event represents only one bit condition, then Baud is the same as bits per second. When each signal event represents other than one bit, Baud does not equal bits per second.

Bell Operating Company (BOC)
Bell Systems Operating Company (BSOC)
Any of the 24 AT&T affiliated companies providing local service.

Bell System
The aggregate of AT&T's 24 associated telephone companies, Long Lines, Western Electric, and Bell Labs.

Billing Number
The MCI term for the number which identifies a customer on a billing location level, assigned to Network Service Customer (by COMS). Assigned for each unique customer name and billing

location. For internal use only.

Binary
A number system that uses only two characters ("0" and "1").

Bit
A binary digit. The smallest unit of coded information.

Bits per Second (BPS)
The rate at which data transmission is measured.

Blocked Calls
Attempted calls that are not connected because (1) all lines to the central offices are in use; or (2) all connecting connecting paths through the PBX/switch are in use.

Blocked ANI
ANI prohibited from completing a call over the MCI network.

Break
A means of interrupting transmission, a momentary interruption of a circuit.

Broadband
A transmission facility having a bandwidth of greater then 20 kHz.

Bus
A heavy conductor, or group of conductors, to which several units of the same type of equipment may be connected.

Busy
The condition in which facilities over which a call is to be connected are already in use.

Busy Hour
The time of day when phone lines are most in demand.

Busy Tone
A single that is interrupted at 60 ipm (impulses per minute) rate to indicate that the terminal point of a call is already in use.

Byte
A group of binary digits that are processed by a computer as a unit.

Carrier
High frequency current that can be modulated with voice or digital signals for bulk transmission via cable or radio circuits.

Carrier System
A system for providing several communications channels over a single path.

Cathode Ray Tube (CRT)
The "television-like" screen used to display the output from a computer.

Cellular Mobile Radio
A system providing exchange telephone service to a station located in an auto or other mobile vehicle, using radio circuits to a base radio station which covers a specific geographical area and as the vehicle moves from one area to another, different base radio stations handle the call.

Central Office
A telephone switching center that provides local access to the public network. Sometimes referred to as: Class 5 office, end

office, or Local Dial Office.

Centrex, CO
PBX Service provided by a switch located at the telephone company central office.

Centrex, CU
A variation on Centrex CO provided by a telephone company maintained "Central Office" type switch located at the customer's premises.

Central Processing Unit (CPU)
The control unit within a computer which handles all the intelligent functions of the systems. In a telephone switch, directs all potions of the system to carry out their appropriate functions. Synonym: Common Control.

Channel
A communication path via a carrier or microwave radio.

Character
Any letter, digit, or special symbol. In data transmission would be represented by a specific code made up of a group of binary digits.

Circuit
A path for the transmission of electromagnetic signals to include all conditioning and signaling equipment. Synonym: Facility

Circuit Switching
A switching system that completes a dedicated transmission path from sender to receiver at the time of transmission.

Class of Service / Class Mark (COS)
A subgrouping of telephone customers or users for the sake of rate distinction or limitation of service.

Coaxial Cable
A cable having several coaxial lines under a single protective sheath. Usually used as a high capacity carrier in urban areas between interexchange and toll offices.

CODEC
Coder-Decoder. Used to convert analog signals to digital form for transmission over a digital median and back again to the original analog form.

Common Carrier
A government regulated private company that provides the general public with telecommunications services and facilities.

Common Channel Interoffice Signalling (CCIS)
A digital technology used by AT&T to enhance their Integrated Services Digital Network. It uses a separate data line to route interoffice signals to provide faster call set-up and more efficient use of trunks.

Common Control Switching Arrangement (CCSA)
An arrangement for telecommunicationsnetworks in which common controlled switching machines are used to route traffic over network routes and access lines. The switching machine may be shared with other users and is maintained by the telephone company.

Computer Port / TKI Port
The interface through which the computer connects to the communications circuit.

Conditioning Equipment
Equipment modifications or adjustments necessary to match

transmission levels and impedances and which equalizes transmission and delay to bring circuit losses, levels, and distortion within established standards.

Configuration
The combination of long-distance services and/or equipment that make up a communications system.

Control Unit (CU)
The central processor of a telephone switching device.

Corporate ID Number
The MCI term for the number which identifies a customer on a corporate level. (Not all MCI customers have this).

Cost Component
The price of each type of long distance service and/or equipment that constitutes a configuration.

Cost per Hour (CPH)
Total cost of different services divided by total holding time (in minutes).

Cross Connection
The wire connections running between terminals on the two sides of a distribution frame, or between binding posts in a terminal.

Cross Talk
The unwanted energy (speech or tone) transferred from one circuit to another circuit.

Customer Owned and Maintained (COAM)
Customer provided communications apparatus, and their associated wiring.

Customer Premise Equipment (CPE)
Telephone equipment, usually including wiring located within the customer's part of a building.

Cut
To transfer a service from one facility to another.

Cut Through
The establishment of a complete path for signaling and/or audio communications.

Data
Any representation, such as characters to which a meaning is assigned.

Data Communications
The movement of coded information by means of electronic transmission systems.

Data Set
A device which converts data into signals suitable for transmission over communications lines.

Data Terminal
A station in a system capable of sending and/or receiving data signals.

Decibel (db)
A unit of measurement represented as a ratio of two voltages, currents or powers and is used to measure transmission loss or gain.

Delay Dial
A dialing configuration whereby local dial equipment will wait until it receives the entire telephone number before seizing a

circuit to transmit the call.

Delta Modulation (DM)
A variant of pulse code modulation whereby a code representing the difference between the amplitude of a sample and the amplitude of a previous one is sent. Operates well in the presence of noise, but requires a wide frequency band.

Demodulation
The process of retrieving data from a modulated signal.

Dial Level
The selection of stations or services associated with a PBX using a one to four digit code (e.g., dialing 9 for access to outside dial tone).

Dial Pulsing
The transmitting of telephone address signals by momentarily opening a DC circuit a number of times corresponding to the decimal digit which is dialed.

Dial Repeating Tie Line
Dial Repeating Tie Trunk
A tie line which permits direct station to station calling without use of the attendant.

Dial Selective Signaling
A multipoint network in which the called party is selected by a prearranged dialing code.

Dial Tone
A tone indicating that automatic switching equipment is ready to receive dial signals.

Dialing Plan
A description of the dialing arrangements for customer use on a networks.

Digital
Referring to the use of digits to formulate and solve problems, or to encode information.

Dimension Custom Telephone Service (DCTS)
AT&T's electronically programmable telephone station sets which use special buttons to access PBX features.

Direct Distance Dialing (DDD)
A toll service that permits customers to dial their own long distance call without the aid of an operator.

Direct Inward Dialing (DID)
A PBX or CENTREX feature that allows a customer outside the system to directly dial a station within the system.

Direct Outward Dialing
A PBX or CENTREX feature that allows a station user to gain direct access to an exchange network.

Drop
That direction of a circuit which looks towards the local operator.

Dry Circuit
A circuit which transmits voice signals and carries no direct current.

Dual Tone Multi Frequency (DTMF)
Also know as Touch Tone. A type of signaling which emits two distinct frequencies for each indicated digit.

Duplex
Simultaneous two-way independent transmission.

DX Signaling
A long-range bidirectional signaling method using paths derived from transmission cable pairs. It is based on a balanced and symmetrical circuit that is identical at both ends. This circuit presents an E&M lead interface to connecting circuits.

This concludes Part 1 Volume I of the MCI Telecommunications Glossary. Look for more G-philes from The MCI School of Telecommunications Management Reference Guide coming soon.

This has been a 2600 Club production
Thanx to Taran King

Electronic Toll Fraud Devices

Typed and Uploaded by
Lex Luthor

This phile is designed to identify various kinds of ETF (electronic toll fraud) devices and to describe their operation, according to a booklet put out by Bell entitled: the investigation and prosecution of electronic toll fraud devices. (For official use only).

There are several different types of electronic equipment which may be generally classified as ETF devices. The most significant is the "blue box". The characteristics of each type of device are discussed below.

Blue Box

The "blue box" was so named because of the color of the first one found. The design and hardware used in the blue box is fairly sophisticated, and its size varies from a large piece of apparatus to a miniaturized unit that is approximately the size of a "king size" package of cigarettes. The blue box contains 12 or 13 buttons or switches that emit multi-frequency tones characteristic of the tones used in the normal operation of the telephone toll (long distance) switching network. The blue box enables its user to originate fraudulent ("free") toll calls by circumventing toll billing equipment. The blue box may be directly connected to a phone line, or it may be acoustically coupled to a telephone handset by placing the blue box's speaker next to the transmitter or the telephone handset. The operation of a blue box will be discussed in more detail below.

To understand the nature of a fraudulent blue box call, it is necessary to understand the basic operation of the direct distance dialing (ddd) telephone network. When a ddd call is properly originated, the calling number is identified as an integral part of establishing the connection. This may be done either automatically or, in some cases, by an operator asking the calling party for his telephone number.

This information is entered on a tape in the automatic message accounting (ama) office. This tape also contains the number assigned to the trunk line over which the call is to be sent. The information relating to the call contained on the tape includes: called number, calling number, time of call. The time of disconnect at the end of the call is also recorded.

Although the tape contains info with respect to many different calls, the various data entries with respect to a single call are eventually correlated to provide billing info for use by your bell's accounting department.

The typical blue box user usually dials a number that will route the call into the telephone network without charge. For example, the user will very often call a well-known inwats (toll-free) customer's number. The blue box user, after gaining this access to the network and, in effect, "seizing" control and complete dominion over the line, operates a key on the blue box which emits a 2600 hertz (cycles per second) tone. This tone causes the switching equipment to release the connection to the inwats customer's line. The 2600Hz tone is a signal that the calling party has hung up. The blue box simulates this condition. However, in fact the local trunk on the calling party's end is still connected to the toll network. The blue box user now operates the "KP" (key pulse) key on the blue box to notify the toll switching equipment that switching signals are about to be emitted. The user then pushes the "number" buttons on the blue box corresponding to the telephone # being called. After doing so he/she operates the "ST" (start) key to indicate to the switching equipment that signalling is complete. If the call is completed, only the portion of the original call prior to the emission of 2600Hz tone is recorded on the ama tape. The tones emitted by the blue box are not recorded on the ama tape. Therefore, because the original call to the inwats # is toll-free, no billing is rendered in connection with the call.

Although the above is a description of a typical blue box operation using a common method of entry into the network, the operation of a blue box may vary in any one or all of the following respects:

(a) The blue box may include a rotary dial to apply the 2600Hz tone and the switching signals. This type of blue box is called a "dial pulser" or "rotary sf" blue box.

(b) entrance into the ddd toll network may be effected by a pretext call to any other toll-free # such as universal directory assistance (555-1212) or any # in the inwats network, either inter-state or intra-state, working or non-working.

(c) entrance into the ddd toll network may also be in the form of "short haul" calling. A "short haul" call is a call to any # which will result in a lesser amount of toll charges than the charges for the call to be completed by the blue box. For example, a call to birmingham from atlanta may cost $.80 for the first 3 minutes while a call from atlanta to los angeles is $1.85 for 3 minutes. Thus, a short haul, 3-minute call to birmingham from atlanta, switched by use of a blue box to los angeles, would result in a net fraud of $2.65 for a 3 minute call.

(d) a blue box may be wired into the telephone line or acoustically connected to the handset. The blue box may even be built inside a regular touch-tone phone, using the phone's push buttons for the blue box's signalling tones.

(e) a magnetic tape recording may be used to record the blue box tones representative of specific phone #'s. Such a tape recording could be used in lieu of a blue box to fraudulently place calls to the phone #'s recorded on the magnetic tape.

All blue boxes, except "dial pulse" or "rotary sf" blue boxes, must have the following 4 common operating capabilities:

(a) it must have signalling capability in the form of a 2600Hz tone. The tone is used by the toll network to indicate, either by its presence or its absence, an "on hook" (idle) or "off hook" (busy) condition of the trunk.

(b) the blue box must have a "KP" tones that unlocks or readies the multi-frequency receiver at the called end to receive the tones corresponding to the called phone #.

(c) the typical blue box must be able to emit mf tones which are used to transmit phone #'s over the toll network. Each digit of a phone # is represented by a combination of 2 tones. For example, the digit 2 is x-mitted by a combination of 700Hz and 1100Hz.

(d) the blue box must have an "ST" key which consists of a combination of 2 tones that tell the equipment at the called end that all digits have been sent and that the equipment should start switching the call to the called number.

the "dial pulser" or "rotary sf" blue box requires only a dial with a signalling capability to produce a 2600Hz tone.

Black Box

This ETF device is so-named because of the color of the first one found. It varies in size and usually has one or two switches or buttons. Attached to the telephone line of a called party, the black box provides toll-free calling to that party's line. A black box user informs other persons beforehand that they will not be charged for any call placed to him. The user then operates the device causing a "non-charge" condition ("no answer" or "disconnect") to be recorded on the telephone company's billing equipment. A black box is relatively simple to construct and is much less sophisticated than a blue box.

Cheese Box

Its design may be crude or very sophisticated. Its size varies; one was found the size of a half-dollar. A cheese box is used most often by bookmakers or betters to place wagers without detection from a remote location. The device interconnects 2 phone lines, each having different #'s but each terminating at the same location. In effect, there are 2 phones at the same location which are linked together through a cheese box. It is usually found in an unoccupied apartment connected to a phone jack or connecting block. The bookmaker, at some remote location, dials one of the numbers and stays on the line. Various bettors dial the other number but are automatically connected with the bookmaker by means of the cheese box inter-connection. If, in addition to a cheese box, a black box is included in the arrangement, the combined equipment would permit toll-free calling on either line to the other line. If a police raid were conducted at the terminating point of the conversations - the location of the cheese box - there would be no evidence of gambling activity. This device is sometimes difficult to identify. Law enforcement officials have been advised that when unusual devices are found associated with telephone connections the phone company security representatives should be contacted to assist in identification. (This probably would be good for a BBS, especially with the black box set up. And if you ever decided to take the board down, you wouldn't have to change your phone

#. It also makes it so you yourself cannot be traced. I am not sure about calling out from one though)

Red Box

This device it coupled acoustically to the handset transmitter of a single-slot coin telephone. The device emits signals identical to those tones emitted when coins are deposited. Thus, local or toll calls may be placed without the actual deposit of coins.

Phreaker's PhunHouse
The Traveler

Brainstorm BBS
612/345-2815 (300/1200)

Little America
507/289-8211 (300)

Tell 'em Traveler sent ya

The long awaited prequil to Phreaker's Guide has finally arrived. Conceived from the boredom and loneliness that could only be derived from: The Traveler! But now, he has returned in full strength (after a small vacation) and is here to 'World Premiere' the new files everywhere.

Stay cool. This is the prequil to the first one, so just relax. This is not made to be an exclusive ultra elite file, so kinda calm down and watch in the background if you are too cool for it ...

Phreak Dictionary

Here you will find some of the basic but necessary terms that should be known by any phreak who wants to be respected at all ...

Phreak [fr'eek]
1. The action of using mischevious and mostly illegal ways in order to not pay for some sort of telecommunications bill, order, transfer, or other service. It often involves usage of highly illegal boxes and machines in order to defeat the security that is set up to avoid this sort of happening.

[fr'eaking]
v. 2. A person who uses the above methods of destruction and chaos in order to make a better life for all. A true phreaker will not not go against his fellows or narc on people who have ragged on him or do anything termed to be dishonorable to phreaks.

[fr'eek]
n. 3. A certain code or dialup useful in the action of being a phreak. (Example: "I hacked a new metro phreak last night.")

Switching System

[Swich'ing sis'tem]
1. There are 3 main switching systems currently employed in the US, and a few other systems will be mentioned as background.

a) SxS: This system was invented in 1918 and was employed in over half of the country until 1978. It is a very basic system that is a general waste of energy and hard work on the linesman. A good way to identify this is that it requires a coin in the phone booth before it will give you a dial tone, or that no call waiting, call forwarding, or any other such service is available. Stands for: Step by Step

b) XB: This switching system was first employed in 1978 in order to take care of most of the faults of SxS switching. Not only is it more efficient, but it also can support different services in various forms. XB1 is Crossbar Version 1. That is very limited and is hard to distinguish from SxS except by direct view of the wiring involved. Next up was XB4, Crossbar Version 4. With this system, some of the basic things like DTMF that were not available with SxS can be accomplished. For the final stroke of XB, XB5 was created. This is a service that can allow DTMF plus most 800 type services (which were not always available ...) Stands for: Crossbar.

c) ESS: A nightmare in telecom. In vivid color, ESS is a pretty bad thing to have to stand up to. It is quite simple to identify. Dialing 911 for emergencies, and ANI [see ANI below] are the most common facets of the dread system. ESS has the capability to list in a person's caller log what number was called, how long the call took, and even the status of the conversation (modem or otherwise.) Since ESS has been employed, which has been very recently, it has gone through many kinds of revisions. The latest system to date is ESS 11a, that is employed in Washington D.C. for security reasons. ESS is truly trouble for any phreak, because it is 'smarter' than the other systems. For instance, if on your caller log they saw 50 calls to 1-800-421-9438, they would be able to do a CN/A [see Loopholes below] on your number and determine whether you are subscribed to that service or not. This makes most calls a hazard, because although 800 numbers appear to be free, they are recorded on your caller log and then right before you receive your bill it deletes the billings for them. But before that they are open to inspection, which is one reason why extended use of any code is dangerous under ESS. Some of the boxes [see Boxing below] are unable to function in ESS. It is generally a menace to the true phreak. Stands For: Electronic Switching System. because they could appear on a filter somewhere or maybe it is just nice to know them any ways.

a) SSS: Strowger Switching System. First non-operator system available.

b) WES: Western Electronics Switching. Used about 40 years ago with some minor places out west.

Boxing [Boks'-ing]
1. The use of personally designed boxes that emit or cancel electronical impulses that allow simpler acting while phreaking. Through the use of separate boxes, you can accomplish most feats possible with or without the control of an operator.
2. Some boxes and their functions are listed below. Ones marked with '*' indicate that they are not operatable in ESS.

*Black Box Makes it seem to the phone company that the phone was never picked up.

Blue Box Emits a 2600Hz tone that allows you to do such things as stack a trunk line, kick the operator off line, and others.

Red Box Simulates the noise of a quarter, nickel, or dime being dropped into a payphone.

Cheese Box Turns your home phone into a pay phone to throw off traces (a red box is usually needed in order to call out.)

*Clear Box Gives you a dial tone on some of the old SxS payphones without putting in a coin.

Beige Box A simpler produced linesman's handset that allows you to tap into phone lines and extract by eavesdropping, or crossing wires, etc.

Purple Box Makes all calls made out from your house seem to be local calls.

ANI [ANI]
1. Automatic Number Identification. A service available on ESS that allows a phone service [see Dialups below] to record the number that any certain code was dialed from along with the number that was called and print both of these on the customer bill. 950 dialups [see Dialups below] are all designed just to use ANI. Some of the services do not have the proper equipment to read the ANI impulses yet, but it is impossible to see which is which without being busted or not busted first.

Dialups [dy'l'ups]
1. Any local or 800 extended outlet that allows instant access to any service such as MCI, Sprint, or AT&T that from there can be used by handpicking or using a program to reveal other peoples codes which can then be used moderately until they find out about it and you must switch to another code (preferably before they find out about it.)
2. Dialups are extremely common on both senses. Some dialups reveal the company that operates them as soon as you hear the tone. Others are much harder and some you may never be able to identify. A small list of dialups:

1-800-421-9438	(5 digit codes)
1-800-547-6754	(6 digit codes)
1-800-345-0008	(6 digit codes)
1-800-734-3478	(6 digit codes)
1-800-222-2255	(5 digit codes)

3. Codes: Codes are very easily accessed procedures when you call a dialup. They will give you some sort of tone. If the tone does not end in 3 seconds, then punch in the code and immediately following the code, the number you are dialing but strike the '1' in the beginning out first. If the tone does end, then punch in the code when the tone ends. Then, it will give you another tone. Punch in the number you are dialing, or a '9'. If you punch in a '9' and the tone stops, then you messed up a little. If you punch in a tone and the tone continues, then simply dial then number you are calling without the '1'.
4. All codes are not universal. The only type that I know of that is truly universal is Metrophone. Almost every major city has a local Metro dialup (for Philadelphia, (215)351-0100/0126) and since the codes are universal, almost every phreak has used them once or twice. They do not employ ANI in any outlets that I know of, so feel free to check through your books and call 555-1212 or, as a more devious manor, subscribe yourself. Then, never use your own code. That way, if they check up on you due to your caller log, they can usually find out that you are subscribed. Not only that but you could set a phreak hacker around that area and just let it hack away, since they usually group them, and, as a bonus, you will have their local dialup.
5. 950's. They seem like a perfectly cool phreakers dream. They are free from your house, from payphones, from everywhere, and they host all of the major long distance companies (950-1044 <MCI>, 950-1077 <Sprint>, 950-1088 <Skylines>, 950-1033 <Us Telecom>.) Well, they aren't. They were designed for ANI. That is the point, end of discussion.

A phreak dictionary. If you remember all of the things contained on that file up there, you may have a better chance of doing whatever it is you do. This next section is maybe a little more interesting ...

Blue Box Plans

These are some blue box plans, but first, be warned, there have been 2600Hz tone detectors out on operator trunk lines since XB4. The idea behind it is to use a 2600Hz tone for a few very naughty functions that can really make your day lighten up. But first, here are the plans, or the heart of the file:

700	1	2	4	7	11
900	+	3	5	8	12
1100	+	+	6	9	KP
1300	+	+	+	10	KP2
1500	+	+	+	+	ST
	700	900	1100	1300	1500

Stop! Before you diehard users start piecing those little tone tidbits together, there is a simpler method. If you have an Apple-Cat with a program like Cat's Meow IV, then you can generate the necessary tones, the 2600Hz tone, the KP tone, the KP2 tone, and the ST tone through the dial section. So if you have that I will assume you can boot it up and it works, and I'll do you the favor of telling you and the other users what to do with the blue box now that you have somehow constructed it.

The connection to an operator is one of the most well known and used ways of having fun with your blue box. You simply dial a TSPS (Traffic Service Positioning Station, or the operator you get when you dial '0') and blow a 2600Hz tone through the line. Watch out! Do not dial this direct! After you have done that, it is quite simple to have fun with it. Blow a KP tone to start a call, a ST tone to stop it, and a 2600Hz tone to hang up. Once you have connected to it, here are some fun numbers to call with it:

0-700-456-1000	Teleconference (free, because you are the operator!)
(Area code)-101	Toll Switching
(Area code)-121	Local Operator (hehe)
(Area code)-131	Information
(Area code)-141	Rate & Route
(Area code)-181	Coin Refund Operator
(Area code)-11511	Conference operator (when you dial 800-544-6363)

Well, those were the tone matrix controllers for the blue box and some other helpful stuff to help you to start out with. But those are only the functions with the operator. There are other k-fun things you can do with it ...

More Advanced Blue Box Stuff

Oops. Small mistake up there. I forgot tone lengths. Um, you blow a tone pair out for up to 1/10 of a second with another 1/10 second for silence between the digits. KP tones should be sent for 2/10 of a second. One way to confuse the 2600Hz traps is to send pink noise over the channel (for all of you that have decent BSR equalizers, there is major pink noise in there ...) Using the operator functions is the use of the 'inward' trunk line. That is working it from the inside. From the 'outward' trunk, you can do such things as make emergency breakthrough calls, tap into lines, busy all of the lines in any trunk (called 'stacking'), enable or disable the TSPS's, and for some 4a systems you can even re-route calls to anywhere.

All right. The one thing that every complete phreak guide should not be without is blue box plans, since they were once a vital part of phreaking. Another thing that every complete file needs is a complete listing of all of the 800 numbers around so you can have some more fun.

800 Dialup Listings

1-800-345-0008	(6)	1-800-547-6754	(6)
1-800-245-4890	(4)	1-800-327-9136	(4)
1-800-526-5305	(8)	1-800-858-9000	(3)
1-800-437-9895	(7)	1-800-245-7508	(5)
1-800-343-1844	(4)	1-800-322-1415	(6)
1-800-437-3478	(6)	1-800-325-7222	(6)

All right, set Cat Hacker 1.0 on those numbers and have a fuck of a day. That is enough with 800 codes, by the time this gets around to you I dunno what state those codes will be in, but try them all out anyways and see what you get. On some 800 services now, they have an operator who will answer and ask you for your code, and then your name. Some will switch back and forth between voice and tone verification, you can never be quite sure which you will be up against.

Armed with this knowledge you should be having a pretty good time phreaking now. But class isn't over yet, there are still a couple important rules that you should know. If you hear continual clicking on the line, then you should assume that an operator is messing with something, maybe even listening in on you. It is a good idea to call someone back when the phone starts doing that. If you were using a code, use a different code and/or service to call him back.

A good way to detect if a code has gone bad or not is to listen when the number has been dialed. If the code is bad you will probably hear the phone ringing more clearly and more quickly than if you were using a different code. If someone answers voice to it then you can immediately assume that it is an operative for whatever company you are using. The famed '311311' code for Metro is one of those. You would have to be quite stupid to actually respond, because whoever you ask for the operator will always say 'He's not in right now, can I have him call you back?' and then they will ask for your name and phone number. Some of the more sophisticated companies will actually give you a carrier on a line that is supposed to give you a carrier and then just have garbage flow across the screen like it would with a bad connection. That is a feeble effort to make you think that the code is still working and maybe get you to dial someone's voice ... a good test for the carrier trick is to dial a number that will give you a carrier that you have never dialed with that code before, that will allow you to determine whether the code is good or not.

For our next section, a lighter look at some of the things that a phreak should not be without. A vocabulary. A few months ago, it was a quite strange world for the modem people out there. But now, a phreaker's vocabulary is essential if you wanna make a good impression on people when you post what you know about certain subjects.

Vocabulary

- Do not misspell except certain exceptions:

  phone -> fone
  freak -> phreak

- Never substitute 'z's for 's's. (i.e. codez -> codes)
- Never leave many characters after a post (i.e. Hey Dudes!#!@#@!#!@)

- NEVER use the 'k' prefix (k-kool, k-rad, k-whatever)
- Do not abbreviate. (I got lotsa wares w/ docs)
- Never substitute '0' for 'o' (r0dent, l0zer).
- Forget about ye old upper case, it looks ruggyish.

All right, that was to relieve the tension of what is being drilled into your minds at the moment ... now, however, back to the teaching course. Here are some things you should know about phones and billings for phones, etc.

LATA

Local Access Transference Area. Some people who live in large cities or areas may be plagued by this problem. For instance, let's say you live in the 215 area code under the 542 prefix (Ambler, Fort Washington). If you went to dial in a basic Metro code from that area, for instance, 351-0100, that might not be counted under unlimited local calling because it is out of your LATA. For some LATA's, you have to dial a '1' without the area code before you can dial the phone number. That could prove a hassle for us all if you didn't realize you would be billed for that sort of call. In that way, sometimes, it is better to be safe than sorry and phreak.

The Caller Log

In ESS regions, for every household around, the phone company has something on you called a Caller Log. This shows every single number that you dialed, and things can be arranged so it showed every number that was calling to you. That's one main disadvantage of ESS, it is mostly computerized so a number scan could be done like that quite easily. Using a dialup is an easy way to screw that, and is something worth remembering. Anyways, with the caller log, they check up and see what you dialed. Hmm ... you dialed 15 different 800 numbers that month. Soon they find that you are subscribed to none of those companies. But that is not the only thing. Most people would imagine "But wait! 800 numbers don't show up on my phone bill!". To those people, it is a nice thought, but 800 numbers are picked up on the caller log until right before they are sent off to you. So they can check right up on you before they send it away and can note the fact that you fucked up slightly and called one too many 800 lines.

Right now, after all of that, you should have a pretty good idea of how to grow up as a good phreak. Follow these guidelines, don't show off, and don't take unnecessary risks when phreaking or hacking.

File Level:5

Credits

To The Videosmith for setting me straight on some shit.
To The Linesman for telling me to upload it to his AE line.
To Modern Mutant for making me into a phreaking freak.
To Jack the Nibbler for the basis of the blue box plans.

By using your new k-koool (hehe) phreaking knowledge, call a couple of these BBS's around the country:

Bulletin Board List

215/844-8836	7 Cities of Gold	(3/12)	10megs
307/382-4006	Brainstorm BBS	(3/12)	
612/345-2815	Metal Shop	(3/12)	
314/432-0756			

Stay free! And watch out soon for Deep Thought, somewhere in 215, that will be a nice BBS that Ace of Spades and I will run. You will be the first to find out about it, trust me ...

Later,

The Traveler
Zer0-g

Basic Telecommunications
Part I

BIOC Agent 003

How to be a Real Phreak

In the phone phreak society there are certain values that exist in order to be a true phreak, these are best summed up by the magician:

> "Many people think of phone phreaks as slime, out to rip off Bell for all she is worth. Nothing could be

further from the truth! Granted, there are some who get their kicks by making free calls; however, they are not true phone phreaks. Real phone phreaks are 'telecommunications hobbyists' who experiment, play with and learn from the phone system. Occasionally this experimenting, and a need to communicate with other phreaks (with-out going broke), leads to free calls. The free calls are but a small subset of a true phone phreaks activities."

The Phone Phreak's Ten Commandments

Reprinted from tap issue #86. (Tap, room 603, 147 w 42 street, New York, NY 10036) send a SASE for their info sheet and tell them that Bioc Agent 003 told you about it.)

i. box thou not over thine home telephone wires, for those who doest must surely bring the wrath of the chief special agent down upon thy heads.

ii. speakest thou not of important matters over thine home telephone wires, for to do so is to risk thine right of freedom.

iii. use not thine own name when speaking to other phreaks, for that every third phreak is an FBI agent is well known.

iv. let not overly many people know that thy be a phreak, as to do so is to use thine own self as a sacrificial lamb.

v. if thou be in school, strive to get thin self good grades, for the authorities well know that scholars never break the law.

vi. if thou workest, try to be a employee, and impressest thine boss with thine enthusiasm, for important employees are often saved by their own bosses.

vii. storest thou not thine stolen goods in thine own home, for those who do are surely non-believers in the Bell system security forces, and are not long for this world.

viii. attractest thou not the attention of the authorities, as the less noticeable thou art, the better.

ix. makest sure thine friends are instant amnesiacs and will not remember that thou have called illegally, for their cooperation with the authorities will surely lessen thine time for freedom on this earth.

x. supportest thou tap, as it is thine newsletter, and without it, thy work will be far more limited.

CN/A Numbers

Customer name & address bureaus exist so that authorized Bell employees may obtain the name & address of any customer in the Bell system by giving the CN/A operator the customer's tel-#. All customers are maintained on file including unlisted #'s. These bureaus have many uses for phreaks.

Here is how an employee might go about calling CN/A:

> "hi, this is john doe from the miami residential service center, can I have the customers name at (123) 555-1212."

The employees usually use these for checking who belongs to a # that someone claimed they didn't call.if you sound cheery and natural the operator will never ask any questions. If you don't sound like a mature adult, don't use it! Always practice first & so you don't screw up and make the operator suspicious. Use name that sounds real, not your pirate name either! Also say that you are fro a city that is far away from the one that you are calling.

The CN/A number for the ny area & vicinity (212, 315, 516, 518, 607, 716, & 914), is 518/471-8111, and is open during business hours. Don't abuse it!

AT&T Newslines

AT&T newslines are numbers at area phone offices that telco employees call to find out the latest info on new technology, stocks, etc. The recorded reports range from very boring to very interesting.

Here are a few of the numbers:

*(201) 483-3800	nj	(518) 471-2272	ny
(203) 771-4920	cn	(717) 255-5555	pa
(212) 393-2151	ny	(717) 787-1031	pa
(516) 234-9941	ny	*(914) 948-8100	ny

* These numbers are not always up!

Some of these numbers are toll-free, but you can't always count on it.
Numbers from other areas are available by request from Bioc Agent 003.

ANI Numbers

ANI numbers identify the phone number that you are calling from. It is useful when playing in cans (those big silver boxes on telephone poles) to find out the # of the line. It is also good to find out the # of a phone that doesn't have it printed on it. In the 914 area code the ANI # is 990. If you just have to dial the last 4 digits for a local #, ie congers (268), dial 1-990-1111, where 1111 are dummy digits there is also a less useful type of ANI# which will identify the area code & exchange. It is nxx-9901, where 'nxx' is the exchange. In the 212 & 516 area codes the ANI # is 958.

Phreak Newsletter

Tap is the "official" phone phreak newsletter, and has existed since 1971. Each 4 page issue is crammed full of information on phone phreaking, computer phreaking, free gas, free electricity, free postage, breaking & entering info, etc. It is largely phone phreak oriented, however.

A 10 issue subscription costs $8.00, if you get a bulk rate sealed envelope subscription. I would recommend the first class subscription, which is $10.

As of this writing (7-16-83), the current issue is #86, and issue #50 is 8 pages instead of the usual 4. Back issues are $0.75 each, and issue #50 is $1.50. A brief index to the first 80 issues is available for a sase, or free with a subscription order. Tap is non-profit, and in desperate need of material (articles), money, and volunteers.

Tap
Room 603
147 west 42nd Street
New York, NY 10036

Believe me: it will be the best $10 you will ever spend ...

Black Box

The black box is a device that attached to a called parties phone that allows him/her to receive free long distance calls from friends who call.

You only need 2 parts: a spst toggle switch and a 10,000 ohm (10 k), 1/2 watt, 10% resistor. Any electronics place should have these.

Now, cut two pieces of wire, about 6 inches, and attach these to the two screws on the switch. Turn your normal ddside down and unscrew the 2 screws. Locate the "f" and "rr" screws on the network box. Wrap the resistor between these 2 screws and make sure that the wires touch only the proper terminals! Now connect one wire from the switch to the rr terminal. Finally, attach the remaining wire to the green wire (disconnect it from its terminal). Now bring the switch out the rear of the phone and close it up. Put the switch in a position where you get a dial tone, mark this normal. Mark the other side free.

When your friends call (at a prearranged time), quickly lift & drop the receiver as fast as possible. This will stop the ringing, if not try again. It is very important that you do it fast! Now put the switch in the free position and pick up the phone. Keep all calls short & under 15 minutes.

When someone calls you long-distance, they are billed from the moment you answer. The telco knows when you answer due to a certain amount of voltage that flows when you pick up the phone. However, the resistor cuts down on the voltage so it is below the billing range but sufficient enough to operate the mouthpiece. Answering the phone for a fraction of a second stops the ring but it is not enough for billing to start. If the phone is answered for even one full second, billing will start and you will be cut off when you hang up and switch to free.

Warning: Bell can randomly look for black boxes so be careful!

```
 _____________________________________
|                                      |
---Blue Wire-->>F<                     |
|              | |                     |
--White Wire---/ |                     |
|                |                     |
|            Resistor                  |
|                |                     |
|                |                     |
|              >RR<-------Switch--\    |
|                                 |    |
----Green Wire--------------------/    |
|                                      |
|_____________________________________|
```

Dial Locks

Have you ever been in an office or somewhere and wanted to make a free fone call but some asshole put a lock on the fone to prevent out-going calls? Fret no more phellow phreaks, for every system can be beaten with a little knowledge!

There are two ways to beat this obstacle, first pick the lock, I don't have the time to teach locksmithing so we go to the second method which takes advantage of telephone electronics.

To be as simple as possible, when you pick up the fone you complete a circuit know as a local loop. When you hang-up you break the circuit. When you dial (pulse) it also breaks the circuit but not long enough to hang up! So you can "push-dial." to do this you >>> rapidly <<< depress the switchhook.

For example, to dial an operator (and then give her the number you want called) >>> rapidly <<< & >>> evenly <<< depress the switchhook 10 times. To dial 634-1268, depress 6 x's pause, then 3 x's, pause, then 4x's, etc. It takes a little practice but you'll get the hang of it. Try practicing with your own # so you'll get a busy tone when right. It'll also work on touch-tone(tm) since a dtmf line will also accept pulse. Also, never depress the switchhook for more than a second or it'll hang-up!

Finally, remember that you have just as much right to that fone as the asshole who put the lock on it!

Exchange Scanning

Almost every exchange in the Bell system has test #'s and other "goodies" such as loops with dial-ups. These "goodies" are usually found between 9900 and 9999 in your local exchange. If you have the time and initiative, scan your exchange and you may become lucky!

here are my findings in the 914-268 exchange:

9900	ANI (see separate bulletin)
9901	ANI (see separate bulletin)
9927	osc. Tone (possible tone side of a loop)
9936	voice # to the telco central office
9937	voice # to the telco central office
9941	computer (digital voice transmission?)
9960	osc. Tone (tone side loop) may also be a computer in some exchanges
9961	no response (other end of loop?)
9962	no response (other end of loop?)
9963	no response (other end of loop?)
9966	computer (see 9941)
9968	tone that disappears - responds to certain touch-tone keys

Most of the numbers between 9900 & 9999 will ring or go to a "What #, please?" operator.

Have phun and remember it's only a local call!

Touch-tone & Free Calls

There are several ways to make free calls (sprint, MCI, etc.) using a rotary phone. They are:

1. Use a number that accepts voice as well as dtmf. Such a # is (800) 521-8400. As of writing this, a code was 00717865.

   If using voice, wait for the computer to say, "authorization #, please." then say each digit slowly, it will beep after each digit is said. After every group of digits, it will repeat what you have said, then say yes if it is correct, otherwise say no. If the access code is correct, it will thank you and ask for the destination #, then say the area code + number as above. Another such # is (800) 245-8173, which has a 6 digit access code. (Note: if using touch-tone on this #, enter the code immediately after the tone stops.)

2. Hook up a touch-tone fone into your rotary fone. Attach the red wire from the touch-tone fone to the "r" terminal inside the fone on the network box. Then hook the green wire to the "b" terminal. To use this dial the # using rotary & then use the touch-tone for the codes. (Don't hang up the rotary fone while doing this though!) if this doesn't work then reverse the 2 wires.

   note if your line can accept touch-tone but you have a rotary fone then you can hook up a tone fone directly for all calls but this usually isn't the case (such as radio shack's 43-138).

Other Alternatives

4. Use a charge-a-call fone. (These also make great extensions if you remove it using a hex wrench with a hole in the middle on the center screw!) - (these fones, for the benefit of those who don't know, are blue with no coin slots).

5. Use a pay fone that wants your money before the dial tone. Put in your dime, dial the #; if it's an 800 # then your dime will come back, immediately put a dime back in (it'll come back when you hang up!) if it is a tone first fone and it disconnects the keypad (some don't) then find another fone.

Chapter 2

Well now we know a little vocabulary, and now its into history, Phreak history. Back at MIT in 1964 arrived a student by the name of Stewart Nelson, who was extremely interested in the telephone. Before entering MIT, he had built autodialers, cheese boxes, and many more gadgets. But when he came to MIT he became even more interested in "fone-hacking" as they called it. After a little while he naturally started using the PDP-1, the schools computer at that time, and from there he decided that it would be interesting to see whether the computer could generate the frequencies required for blue boxing. The hackers at MIT were not interested in ripping off Ma Bell, but just exploring the telephone network. Stew (as he was called) wrote a program to generate all the tones and set off into the vast network.

Now there were more people phreaking than the ones at MIT. Most people have heard of Captain Crunch (No not the cereal), he also discovered how to take rides through the fone system, with the aid of a small whistle found in a cereal box (can we guess which one?). By blowing this whistle, he generated the magical 2600Hz and into the mouthpiece it sailed, giving him complete control over the system. I have heard rumors that at one time he made about 1/4 of the calls coming out of San Francisco. He got famous fast. He made the cover of people magazine and was interviewed several times (as you'll soon see). Well he finally got caught after a long adventurous career. After he was caught he was put in jail and was beaten up quite badly because he would not teach other inmates how to box calls. After getting out, he joined Apple computer and is still out there somewhere.

Then there was Joe the Whistler, blind form the day he was born. He could whistle a perfect 2600Hz tone. It was rumored phreaks used to call him to tune their boxes.

Well that was up to about 1970, then from 1970 to 1979, phreaking was mainly done by college students, businessmen and anyone who knew enough about electronics and the fone company to make a 555 Ic to generate those magic tones. Businessmen and a few college students mainly just blue box to get free calls. The others were still there, exploring 800#'s and the new ESS systems. ESS posed a big problem for phreaks then and even a bigger one now. ESS was not widespread, but where it was, blue boxing was next to impossible except for the most experienced phreak. Today ESS is installed in almost all major cities and blue boxing is getting harder and harder.

1978 marked a change in phreaking, the Apple][, now a computer that was affordable, could be programmed, and could save all that precious work on a cassette. Then just a short while later came the Apple Cat modem. With this modem, generating all blue box tones was easy as writing a program to count form one to ten (a little exaggerated). Pretty soon programs that could imitate an operator just as good as the real thing were hitting the community, TSPS and Cat's Meow, are the standard now and are the best.

1982-1986: LD services were starting to appear in mass numbers. People now had programs to hack LD services, telephone exchanges, and even passwords. By now many phreaks were getting extremely good and BBS's started to spring up everywhere, each having many documentations on phreaking for the novice. Then it happened, the movie War Games was released and mass numbers of sixth grade to all ages flocked to see it. The problem wasn't that the movie was bad, it was that now EVERYONE wanted to be a hacker/phreak. Novices came out in such mass numbers, that bulletin boards started to be busy 24 hours a day. To this day, they still have not recovered. Other problems started to occur, novices guessed easy passwords on large government computers and started to play around ... Well it wasn't long before they were caught, I think that many people remember the 414-hackers. They were so stupid as to say "yes" when the computer asked them whether they'd like to play games. Well at least it takes the heat off the real phreaks/hacker/krackers.

After a little history, how about a little thrill? I don't know if this story is true but it sure is as bad as shit!

Secrets of the Little Blue Box
by Ron Rosenbaum

Typed by One Farad Cap/AAG
(First of four files)

A story so incredible it may even make you feel sorry for the phone company.

Printed in the October 1971 issue of Esquire Magazine. If you happen to be in a library and come across a collection of Esquire magazines, the October 1971 issue is the first issue printed in the smaller format. The story begins on page 116 with a picture of a blue box.

One Farad Cap, Atlantic Anarchist Guild

The Blue Box Is Introduced
Its Qualities Are Remarked (Part 1)

I am in the expensively furnished living room of Al Gilbertson (His real name has been changed.), the creator of the "blue box." Gilbertson is holding one of his shiny black-and-silver "blue boxes" comfortably in the palm of his hand, pointing out the thirteen little red push buttons sticking up from the console. He is dancing his fingers over the buttons, tapping out discordant beeping electronic jingles. He is trying to explain to me how his little blue box does nothing less than place the entire telephone system of the world, satellites, cables and all, at the service of the blue-box operator, free of charge.

"That's what it does. Essentially it gives you the power of a super operator. You seize a tandem with this top button," he presses the top button with his index finger and the blue box emits a high-pitched cheep, "and like that" -- cheep goes the blue box again -- "you control the phone company's long-distance switching systems from your cute little Princes phone or any old pay phone. And you've got anonymity. An operator has to operate from a definite location: the phone company knows where she is and what she's doing. But with your beeper box, once you hop onto a trunk, say from a Holiday Inn 800 (toll-free) number, they don't know where you are, or where you're coming from, they don't know how you slipped into their lines and popped up in that 800 number. They don't even know anything illegal is going on. And you can obscure your origins through as many levels as you like. You can call next door by way of White Plains, then over to Liverpool by cable, and then back here by satellite. You can call yourself from one pay phone all the way around the world to a pay phone next to you. And you get your dime back too."

"And they can't trace the calls? They can't charge you?"

"Not if you do it the right way. But you'll find that the free-call thing isn't really as exciting at first as the feeling of power you get from having one of these babies in your hand. I've watched people when they first get hold of one of these things and start using it, and discover they can make connections, set up crisscross and zigzag switching patterns back and forth across the world. They hardly talk to the people they finally reach. They say hello and start thinking of what kind of call to make next. They go a little crazy." He looks down at the neat little package in his palm. His fingers are still dancing, tapping out beeper patterns.

"I think it's something to do with how small my models are. There are lots of blue boxes around, but mine are the smallest and most sophisticated electronically. I wish I could show you the prototype we made for our big syndicate order."

He sighs. "We had this order for a thousand beeper boxes from a syndicate front man in Las Vegas. They use them to place bets coast to coast, keep lines open for hours, all of which can get expensive if you have to pay. The deal was a thousand blue boxes for $300 apiece. Before then we retailed them for $1500 apiece, but $300,000 in one lump was hard to turn down. We had a manufacturing deal worked out in the Philippines. Everything ready to go. Anyway, the model I had ready for limited mass production was small enough to fit inside a flip-top Marlboro box. It had flush touch panels for a keyboard, rather than these unsightly buttons, sticking out. Looked just like a tiny portable radio. In fact, I had designed it with a tiny transistor receiver to get one AM channel, so in case the law became suspicious the owner could switch on the radio part, start snapping his fingers, and no one could tell anything illegal was going on. I thought of everything for this model -- I had it lined with a band of thermite which could be ignited by radio signal from a tiny button transmitter on your belt, so it could be burned to ashes instantly in case of a bust. It was beautiful. A beautiful little machine. You should have seen the faces on these syndicate guys when they came back after trying it out. They'd hold it in their palm like they never wanted to let it go, and they'd say, 'I can't believe it. I can't believe it.' You probably won't believe it until you try it."

The Blue Box Is Tested
Certain Connections Are Made

About eleven o'clock two nights later Fraser Lucey has a blue box in the palm of his left hand and a phone in the palm of his right. He is standing inside a phone booth next to an isolated shut-down motel off Highway 1. I am standing outside the phone booth.

Fraser likes to show off his blue box for people. Until a few weeks ago when Pacific Telephone made a few arrests in his city, Fraser Lucey liked to bring his blue box (This particular blue box, like most blue boxes, is not blue. Blue boxes have come to be called "blue boxes" either because 1) The first blue box ever confiscated by phone-company security men happened to be blue, or 2) To distinguish them from "black boxes." Black boxes are devices, usually a resistor in series, which, when attached to home phones, allow all incoming calls to be made without charge to one's caller.) to parties. It never failed: a few cheeps from his device and Fraser became the center of attention at the very hippest of gatherings, playing phone tricks and doing request numbers for hours. He began to take orders for his manufacturer in Mexico. He became a dealer.

Fraser is cautious now about where he shows off his blue box. But he never gets tired of playing with it. "It's like the first time every time," he tells me.

Fraser puts a dime in the slot. He listens for a tone and holds the receiver up to my ear. I hear the tone. Fraser begins describing, with a certain practiced air, what he does while he does it. "I'm dialing an 800 number now. Any 800 number will do. It's toll free. Tonight I think I'll use the -- (he names a well-know rent-a-car company) 800 number. Listen, It's ringing. Here, you hear it? Now watch." He places the blue box over the mouthpiece of the phone so that the one silver and twelve black push buttons are facing up toward me. He presses the silver button -- the one at the top -- and I hear that high-pitched beep. "That's 2600 cycles per second to be exact," says Lucey. "Now, quick. listen." He shoves the earpiece at me. The ringing has vanished. The line gives a slight hiccough, there is a sharp buzz, and then nothing but soft white noise.

"We're home free now," Lucey tells me, taking back the phone and applying the blue box to its mouthpiece once again. "We're up on a tandem, into a long-lines trunk. Once you're up on a tandem, you can send yourself anywhere you want to go." He decides to check out London first. He chooses a certain pay phone located in Waterloo Station. This particular pay phone is popular with the phone-phreaks network because there are usually people walking by at all hours who will pick it up and talk for a while.

He presses the lower left-hand corner button which is marked "KP" on the face of the box. "That's Key Pulse. It tells the tandem we're ready to give it instructions. First I'll punch out KP 182 START, which will slide us into the overseas sender in White Plains." I hear a neat clunk-cheep. "I think we'll head over to England by satellite. Cable is actually faster and the connection is somewhat better, but I like going by satellite. So I just punch out KP Zero 44. The Zero is supposed to guarantee a satellite connection and 44 is the country code for England. Okay ... we're there. In Liverpool actually. Now all I have to do is punch out the London area code which is 1, and dial up the pay phone. Here, listen, I've got a ring now."

I hear the soft quick purr-purr of a London ring. Then someone picks up the phone.

"Hello," says the London voice.

"Hello. Who's this?" Fraser asks.

"Hello. There's actually nobody here. I just picked this up while I was passing by. This is a public phone. There's no one here to answer actually."

"Hello. Don't hang up. I'm calling from the United States."

"Oh. What is the purpose of the call? This is a public phone you know."

"Oh. You know. To check out, uh, to find out what's going on in London. How is it there?"

"Its five o'clock in the morning. It's raining now."

"Oh. Who are you?"

The London passerby turns out to be an R.A.F. enlistee on his way back to the base in Lincolnshire, with a terrible hangover after a thirty-six-hour pass.

He and Fraser talk about the rain. They agree that it's nicer when it's not raining. They say good-bye and Fraser hangs up. His dime returns with a nice clink.

"Isn't that far out," he says grinning at me. "London, like that."

Fraser squeezes the little blue box affectionately in his palm. "I told ya this thing is for real. Listen, if you don't mind I'm gonna try this girl I know in Paris. I usually give her a call around this time. It freaks her out. This time I'll use the -- (a different rent-a-car company) 800 number and we'll go by overseas cable, 133; 33 is the country code for France, the 1 sends you by cable. Okay, here we go ... Oh damn. Busy. Who could she be talking to at this time?"

A state police car cruises slowly by the motel. The car does not stop, but Fraser gets nervous. We hop back into his car and drive ten miles in the opposite direction until we reach a Texaco station locked up for the night. We pull up to a phone booth by the tire pump. Fraser dashes inside and tries the Paris number. It is busy again.

"I don't understand who she could be talking to. The circuits may be busy. It's too bad I haven't learned how to tap into lines overseas with this thing yet."

Fraser begins to phreak around, as the phone phreaks say. He dials a leading nationwide charge card's 800 number and punches out the tones that bring him the time recording in Sydney, Australia. He beeps up the weather recording in Rome, in Italian of course. He calls a friend in Boston and talks about a certain over-the-counter stock they are into heavily. He finds the Paris number busy again. He calls up "Dial a Disc" in London, and we listen to Double Barrel by David and Ansil Collins, the number-one hit of the week in London. He calls up a dealer of another sort and talks in code. He calls up Joe Engressia, the original blind phone-phreak genius, and pays his respects. There are other calls. Finally Fraser gets through to his young lady in Paris.

They both agree the circuits must have been busy, and criticize the Paris telephone system. At two-thirty in the morning Fraser hangs up, pockets his dime, and drives off, steering with one hand, holding what he calls his "lovely little blue box" in the other.

You Can Call Long Distance For Less Than You Think

"You see, a few years ago the phone company made one big mistake," Gilbertson explains two days later in his apartment. "They were careless enough to let some technical journal publish the actual frequencies used to create all their multi-frequency tones. Just a theoretical article some Bell Telephone Laboratories engineer was doing about switching theory, and he listed the tones in passing. At -- (a well-known technical school) I had been fooling around with phones for several years before I came across a copy of the journal in the engineering library. I ran back to the lab and it took maybe twelve hours from the time I saw that article to put together the first working blue box. It was bigger and clumsier than this little baby, but it worked."

It's all there on public record in that technical journal written mainly by Bell Lab people for other telephone engineers. Or at least it was public. "Just try and get a copy of that issue at some engineering-school library now. Bell has had them all red-tagged and withdrawn from circulation," Gilbertson tells me.

"But it's too late. It's all public now. And once they became public the technology needed to create your own beeper device is within the range of any twelve-year-old kid, any twelve-year-old blind kid as a matter of fact. And he can do it in less than the twelve hours it took us. Blind kids do it all the time. They can't build anything as precise and compact as my beeper box, but theirs can do anything mine can do."

"How?"

"Okay. About twenty years ago A.T.&T. made a multi-billion-dollar decision to operate its entire long-distance switching system on twelve electronically generated combinations of twelve master tones. Those are the tones you sometimes hear in the background after you've dialed a long-distance number. They decided to use some very simple tones -- the tone for each number is just two fixed single-frequency tones played simultaneously to create a certain beat frequency. Like 1300 cycles per second and 900 cycles per second played together give you the tone for digit 5. Now, what some of these phone phreaks have done is get themselves access to an electric organ. Any cheap family home-entertainment organ. Since the frequencies are public knowledge now -- one blind phone phreak has even had them recorded in one of the talking books for the blind -- they just have to find the musical notes on the organ which correspond to the phone tones. Then they tape them. For instance, to get Ma Bell's tone for the number 1, you press down organ keys F˜5 and A˜5 (900 and 700 cycles per second) at the same time. To produce the tone for 2 it's F˜5 and C˜6 (1100 and 700 c.p.s). The phone phreaks circulate the whole list of notes so there's no trial and error anymore."

He shows me a list of the rest of the phone numbers and the two electric organ keys that produce them.

"Actually, you have to record these notes at 3 3/4 inches-per-second tape speed and double it to 7 1/2 inches-per-second when you play them back, to get the proper tones," he adds.

"So once you have all the tones recorded, how do you plug them into the phone system?"

"Well, they take their organ and their cassette recorder, and start banging out entire phone numbers in tones on the organ, including country codes, routing instructions, 'KP' and 'Start' tones. Or, if they don't have an organ, someone in the phone-phreak network sends them a cassette with all the tones recorded, with a voice saying 'Number one,' then you have the tone, 'Number two,' then the tone and so on. So with two cassette recorders they can put together a series of phone numbers by switching back and forth from number to number. Any idiot in the country with a cheap cassette recorder can make all the free calls he wants."

"You mean you just hold the cassette recorder up the mouthpiece and switch in a series of beeps you've recorded? The phone thinks that anything that makes these tones must be its own equipment?"

"Right. As long as you get the frequency within thirty cycles per second of the phone company's tones, the phone equipment thinks it hears its own voice talking to it. The original granddaddy phone phreak was this blind kid with perfect pitch, Joe Engressia, who used to whistle into the phone. An operator could tell the difference between his whistle and the phone company's electronic tone generator, but the phone company's switching circuit can't tell them apart. The bigger the phone company gets and the further away from human operators it gets, the more vulnerable it becomes to all sorts of phone phreaking."

A Guide for the Perplexed

"But wait a minute," I stop Gilbertson. "If everything you do sounds like phone-company equipment, why doesn't the phone company charge you for the call the way it charges its own equipment?"

"Okay. That's where the 2600-cycle tone comes in. I better start from the beginning."

The beginning he describes for me is a vision of the phone system of the continent as thousands of webs, of long-line trunks radiating from each of the hundreds of toll switching offices to the other toll switching offices. Each toll switching office is a hive compacted of thousands of long-distance tandems constantly whistling and beeping to tandems in far-off toll switching offices.

The tandem is the key to the whole system. Each tandem is a line with some relays with the capability of signalling any other tandem in any other toll switching office on the continent, either directly one-to-one or by programming a roundabout route through several other tandems if all the direct routes are busy. For instance, if you want to call from New York to Los Angeles and traffic is heavy on all direct trunks between the two cities, your tandem in New York is programmed to try the next best route, which may send you down to a tandem in New Orleans, then up to San Francisco, or down to a New Orleans tandem, back to an Atlanta tandem, over to an Albuquerque tandem and finally up to Los Angeles.

When a tandem is not being used, when it's sitting there waiting for someone to make a long-distance call, it whistles. One side of the tandem, the side "facing" your home phone, whistles at 2600 cycles per second toward all the home phones serviced by the exchange, telling them it is at their service, should they be interested in making a long-distance call. The other side of the tandem is whistling 2600 c.p.s. into one or more long-distance trunk lines, telling the rest of the phone system that it is neither sending nor receiving a call through that trunk at the moment, that it has no use for that trunk at the moment.

"When you dial a long-distance number the first thing that happens is that you are hooked into a tandem. A register comes up to the side of the tandem facing away from you and presents that side with the number you dialed. This sending side of the tandem stops whistling 2600 into its trunk line. When a tandem stops the 2600 tone it has been sending through a trunk, the trunk is said to be "seized," and is now ready to carry the number you have dialed -- converted into multi-frequency beep tones -- to a tandem in the area code and central office you want.

Now when a blue-box operator wants to make a call from New Orleans to New York he starts by dialing the 800 number of a company which might happen to have its headquarters in Los Angeles. The sending side of the New Orleans tandem stops sending 2600 out over the trunk to the central office in Los Angeles, thereby seizing the trunk. Your New Orleans tandem begins sending beep tones to a tandem it has discovered idly whistling 2600 cycles in Los Angeles. The receiving end of that L.A. tandem is seized, stops whistling 2600, listens to the beep tones which tell it which L.A. phone to ring, and starts ringing the 800 number. Meanwhile a mark made in the New Orleans office accounting tape notes that a call from your New Orleans phone to the 800 number in L.A. has been initiated and gives the call a code number. Everything is routine so far.

But then the phone phreak presses his blue box to the mouthpiece and pushes the 2600-cycle button, sending 2600 out from the New Orleans tandem to the L.A. tandem. The L.A. tandem notices 2600 cycles are coming over the line again and assumes that New Orleans has hung up because the trunk is whistling as if idle. The L.A. tandem immediately ceases ringing the L.A. 800 number. But as soon as the phreak takes his finger off the 2600 button, the L.A. tandem assumes the trunk is once again being used because the 2600 is gone, so it listens for a new series of digit tones - to find out where it must send the call.

Thus the blue-box operator in New Orleans now is in touch with a tandem in L.A. which is waiting like an obedient genie to be told what to do next. The blue-box owner then beeps out the ten digits of the New York number which tell the L.A. tandem to relay a call to New York City. Which it promptly does. As soon as your party picks up the phone in New York, the side of the New Orleans tandem facing you stops sending 2600 cycles to you and stars carrying his voice to you by way of the L.A. tandem. A notation is made on the accounting tape that the connection has been made on the 800 call which had been initiated and noted earlier. When you stop talking to New York a notation is made that the 800 call has ended.

At three the next morning, when the phone company's accounting computer starts reading back over the master accounting tape for the past day, it records that a call of a certain length of time was made from your New Orleans home to an L.A. 800 number and, of course, the accounting computer has been trained to ignore those toll-free 800 calls when compiling your monthly bill.

"All they can prove is that you made an 800 toll-free call," Gilbertson the inventor concludes. "Of course, if you're foolish enough to talk for two hours on an 800 call, and they've installed one of their special anti-fraud computer programs to watch out for such things, they may spot you and ask why you took two hours talking to Army Recruiting's 800 number when you're 4-F.

But if you do it from a pay phone, they may discover something peculiar the next day -- if they've got a blue-box hunting program in their computer -- but you'll be a long time gone from the pay phone by then. Using a pay phone is almost guaranteed safe."

"What about the recent series of blue-box arrests all across the country -- New York, Cleveland, and so on?" I asked. "How were they caught so easily?"

"From what I can tell, they made one big mistake: they were seizing trunks using an area code plus 555-1212 instead of an 800 number. Using 555 is easy to detect because when you send multi-frequency beep tones of 555 you get a charge for it on your tape and the accounting computer knows there's something wrong when it tries to bill you for a two-hour call to Akron, Ohio, information, and it drops a trouble card which goes right into the hands of the security agent if they're looking for blue-box user.

"Whoever sold those guys their blue boxes didn't tell them how to use them properly, which is fairly irresponsible. And they were fairly stupid to use them at home all the time.

"But what those arrests really mean is than an awful lot of blue boxes are flooding into the country and that people are finding them so easy to make that they know how to make them before they know how to use them. Ma Bell is in trouble."

And if a blue-box operator or a cassette-recorder phone phreak sticks to pay phones and 800 numbers, the phone company can't stop them?

"Not unless they change their entire nationwide long-lines technology, which will take them a few billion dollars and twenty years. Right now they can't do a thing. They're screwed."

Captain Crunch Demonstrates His Famous Unit (part II)

There is an underground telephone network in this country. Gilbertson discovered it the very day news of his activities hit the papers. That evening his phone began ringing. Phone phreaks from Seattle, from Florida, from New York, from San Jose, and from Los Angeles began calling him and telling him about the phone-phreak network. He'd get a call from a phone phreak who'd say nothing but, "Hang up and call this number."

When he dialed the number he'd find himself tied into a conference of a dozen phone phreaks arranged through a quirky switching station in British Columbia. They identified themselves as phone phreaks, they demonstrated their homemade blue boxes which they called "M-Fers" (for "multi-frequency," among other things) for him, they talked shop about phone-phreak devices. They let him in on their secrets on the theory that if the phone company was after him he must be trustworthy. And, Gilbertson recalls, they stunned him with their technical sophistication.

I ask him how to get in touch with the phone-phreak network. He digs around through a file of old schematics and comes up with about a dozen numbers in three widely separated area codes.

"Those are the centers," he tells me. Alongside some of the numbers he writes in first names or nicknames: names like Captain Crunch, Dr. No, Frank Carson (also a code word for a free call), Marty Freeman (code word for M-F device), Peter Perpendicular Pimple, Alefnull, and The Cheshire Cat. He makes checks alongside the names of those among these top twelve who are blind. There are five checks.

I ask him who this Captain Crunch person is.

"Oh. The Captain. He's probably the most legendary phone phreak. He calls himself Captain Crunch after the notorious Cap'n Crunch 2600 whistle." (Several years ago, Gilbertson explains, the makers of Cap'n Crunch breakfast cereal offered a toy-whistle prize in every box as a treat for the Cap'n Crunch set. Somehow a phone phreak discovered that the toy whistle just happened to produce a perfect 2600-cycle tone. When the man who calls himself Captain Crunch was transferred overseas to England with his Air Force unit, he would receive scores of calls from his friends and "mute" them -- make them free of charge to them -- by blowing his Cap'n Crunch whistle into his end.)

"Captain Crunch is one of the older phone phreaks," Gilbertson tells me. "He's an engineer who once got in a little trouble for fooling around with the phone, but he can't stop. Well, they guy drives across country in a Volkswagen van with an entire switchboard and a computerized super-sophisticated M-F-er in the back. He'll pull up to a phone booth on a lonely highway somewhere, snake a cable out of his bus, hook it onto the phone and sit for hours, days sometimes, sending calls zipping back and forth across the country, all over the world ... "

Back at my motel, I dialed the number he gave me for "Captain Crunch" and asked for G-- T--, his real name, or at least the name he uses when he's not dashing into a phone booth beeping out M-F tones faster than a speeding bullet and zipping phantomlike through the phone company's long-distance lines.

When G-- T-- answered the phone and I told him I was preparing a story for Esquire about phone phreaks, he became very indignant.

"I don't do that. I don't do that anymore at all. And if I do it, I do it for one reason and one reason only. I'm learning about a system. The phone company is a System. A computer is a System, do you understand? If I do what I do, it is only to explore a system. Computers, systems, that's my bag. The phone company is nothing but a computer."

A tone of tightly restrained excitement enters the Captain's voice when he starts talking about systems. He begins to pronounce each syllable with the hushed deliberation of an obscene caller.

"Ma Bell is a system I want to explore. It's a beautiful system, you know, but Ma Bell screwed up. It's terrible because Ma Bell is such a beautiful system, but she screwed up. I learned how she screwed up from a couple of blind kids who wanted me to build a device. A certain device. They said it could make free calls. I wasn't interested in free calls. But when these blind kids told me I could make calls into a computer, my eyes lit up. I wanted to learn about computers. I wanted to learn about Ma Bell's computers. So I build the little device, but I built it wrong and Ma Bell found out. Ma Bell can detect things like that. Ma Bell knows. So I'm strictly rid of it now. I don't do it. Except for learning purposes." He pauses. "So you want to write an article. Are you paying for this call? Hang up and call this number." He gives me a number in a area code a thousand miles away of his own. I dial the number.

"Hello again. This is Captain Crunch. You are speaking to me on a toll-free loop-around in Portland, Oregon. Do you know what a toll-free loop around is?

I'll tell you.

He explains to me that almost every exchange in the country has open test numbers which allow other exchanges to test their connections with it. Most of these numbers occur in consecutive pairs, such as 302 956-0041 and 302 956-0042. Well, certain phone phreaks discovered that if two people from anywhere in the country dial the two consecutive numbers they can talk together just as if one had called the other's number, with no charge to either of them, of course.

"Now our voice is looping around in a 4A switching machine up there in Canada, zipping back down to me," the Captain tells me. "My voice is looping around up there and back down to you. And it can't ever cost anyone money. The phone phreaks and I have compiled a list of many many of these numbers. You would be surprised if you saw the list. I could show it to you. But I won't. I'm out of that now. I'm not out to screw Ma Bell. I know better. If I do anything it's for the pure knowledge of the System. You can learn to do fantastic things. Have you ever heard eight tandems stacked up? Do you know the sound of tandems stacking and unstacking? Give me your phone number. Okay. Hang up now and wait a minute."

Slightly less than a minute later the phone rang and the Captain was on the line, his voice sounding far more excited, almost aroused.

"I wanted to show you what it's like to stack up tandems. To stack up tandems." (Whenever the Captain says "stack up" it sounds as if he is licking his lips.)

"How do you like the connection you're on now?" the Captain asks me. "It's a raw tandem. A raw tandem. Ain't nothin' up to it but a tandem. Now I'm going to show you what it's like to stack up. Blow off. Land in a far away place. To stack that tandem up, whip back and forth across the country a few times, then shoot on up to Moscow.

"Listen," Captain Crunch continues. "Listen. I've got line tie on my switchboard here, and I'm gonna let you hear me stack and unstack tandems. Listen to this. It's gonna blow your mind."

First I hear a super rapid-fire pulsing of the flutelike phone tones, then a pause, then another popping burst of tones, then another, then another. Each burst is followed by a beep-kachink sound.

"We have now stacked up four tandems," said Captain Crunch, sounding somewhat remote. "That's four tandems stacked up. Do you know what that means? That means I'm whipping back and forth, back and forth twice, across the country, before coming to you. I've been known to stack up twenty tandems at a time. Now, just like I said, I'm going to shoot up to Moscow."

There is a new, longer series of beeper pulses over the line, a brief silence, then a ring.

"Hello," answers a far-off voice.

"Hello. Is this the American Embassy Moscow?"

"Yes, sir. Who is this calling?" says the voice.

"Yes. This is test board here in New York. We're calling to check out the circuits, see what kind of lines you've got. Everything okay there in Moscow?"

"Okay?"

"Well, yes, how are things there?"

"Oh. Well, everything okay, I guess."

"Okay. Thank you."

They hang up, leaving a confused series of beep-kachink sounds hanging in mid-ether in the wake of the call before dissolving away.

The Captain is pleased. "You believe me now, don't you? Do you know what I'd like to do? I'd just like to call up your editor at Esquire and show him just what it sounds like to stack and unstack tandems. I'll give him a show that will blow his mind. What's his number?

I ask the Captain what kind of device he was using to accomplish all his feats. The Captain is pleased at the question.

"You could tell it was special, couldn't you?" Ten pulses per second. That's faster than the phone company's equipment. Believe me, this unit is the most famous unit in the country. There is no other unit like it. Believe me."

"Yes, I've heard about it. Some other phone phreaks have told me about it."

"They have been referring to my, ahem, unit? What is it they said? Just out of curiosity, did they tell you it was a highly sophisticated computer-operated unit, with acoustical coupling for receiving outputs and a switch-board with multiple-line-tie capability? Did they tell you that the frequency tolerance is guaranteed to be not more than .05 percent? The amplitude tolerance less than .01 decibel? Those pulses you heard were perfect. They just come faster than the phone company. Those were high-precision op-amps. Op-amps are instrumentation amplifiers designed for ultra-stable amplification, super-low distortion and accurate frequency response. Did they tell you it can operate in temperatures from -55 degrees C to +125 degrees C?"

I admit that they did not tell me all that.

"I built it myself," the Captain goes on. "If you were to go out and buy the components from an industrial wholesaler it would cost you at least $1500. I once worked for a semiconductor company and all this didn't cost me a cent. Do you know what I mean? Did they tell you about how I put a call completely around the world? I'll tell you how I did it. I M-Fed Tokyo inward, who connected me to India, India connected me to Greece, Greece connected me to Pretoria, South Africa, South Africa connected me to South America, I went from South America to London, I had a London operator connect me to a New York operator, I had New York connect me to a California operator who rang the phone next to me. Needless to say I had to shout to hear myself. But the echo was far out. Fantastic. Delayed. It was delayed twenty seconds, but I could hear myself talk to myself."

"You mean you were speaking into the mouthpiece of one phone sending your voice around the world into your ear through a phone on the other side of your head?" I asked the Captain. I had a vision of something vaguely autoerotic going on, in a complex electronic way.

"That's right," said the Captain. "I've also sent my voice around the world one way, going east on one phone, and going west on the other, going through cable one way, satellite the other, coming back together at the same time, ringing the two phones simultaneously and picking them up and whipping my voice both ways around the world back to me. Wow. That was a mind blower."

"You mean you sit there with both phones on your ear and talk to yourself around the world," I said incredulously.

"Yeah. Um hum. That's what I do. I connect the phone together and sit there and talk."

"What do you say? What do you say to yourself when you're connected?"

"Oh, you know. Hello test one two three," he says in a low-pitched voice.

"Hello test one two three," he replied to himself in a high-pitched voice.

"Hello test one two three," he repeats again, low-pitched.

"Hello test one two three," he replies, high-pitched.

"I sometimes do this: Hello Hello Hello Hello, Hello, hello," he trails off and breaks into laughter.

Why Captain Crunch Hardly Ever Taps Phones Anymore

Using internal phone-company codes, phone phreaks have learned a simple method for tapping phones. Phone-company operators have in front of them a board that holds verification jacks. It allows them to plug into conversations in case of emergency, to listen in to a line to determine if the line is busy or the circuits are busy. Phone phreaks have learned to beep out the codes which lead them to a verification operator, tell the verification operator they are switchmen from some other area code testing out verification trunks. Once the operator hooks them into the verification trunk, they disappear into the board for all practical purposes, slip unnoticed into any one of the 10,000 to 100,000 numbers in that central office without the verification operator knowing what they're doing, and of course without the two parties to the connection knowing there is a phantom listener present on their line.

Toward the end of my hour-long first conversation with him, I asked the Captain if he ever tapped phones.

"Oh no. I don't do that. I don't think it's right," he told me firmly. "I have the power to do it but I don't ... Well one time, just one time, I have to admit that I did. There was this girl, Linda, and I wanted to find out ... you know. I tried to call her up for a date. I had a date with her the last weekend and I thought she liked me. I called her up, man, and her line was busy, and I kept calling and it was still busy. Well, I had just learned about this system of jumping into lines and I said to myself, 'Hmmm. Why not just see if it works. It'll surprise her if all of a sudden I should pop up on her line. It'll impress her, if anything.' So I went ahead and did it. I M-Fed into the line. My M-F-er is powerful enough when patched directly into the mouthpiece to trigger a verification trunk without using an operator the way the other phone phreaks have to.

"I slipped into the line and there she was talking to another boyfriend. Making sweet talk to him. I didn't make a sound because I was so disgusted. So I waited there for her to hang up, listening to her making sweet talk to the other guy. You know. So as soon as she hung up I instantly M-F-ed her up and all I said was, 'Linda, we're through.' And I hung up. And it blew her head off. She couldn't figure out what the hell happened.

"But that was the only time. I did it thinking I would surprise her, impress her. Those were all my intentions were, and well, it really kind of hurt me pretty badly, and ... and ever since then I don't go into verification trunks."

Moments later my first conversation with the Captain comes to a close.

"Listen," he says, his spirits somewhat cheered, "listen. What you are going to hear when I hang up is the sound of tandems unstacking. Layer after layer of tandems unstacking until there's nothing left of the stack, until it melts away into nothing. Cheep, cheep, cheep, cheep," he concludes, his voice descending to a whisper with each cheep.

He hangs up. The phone suddenly goes into four spasms: kachink cheep. Kachink cheep kachink cheep kachink cheep, and the complex connection has wiped itself out like the Cheshire cat's smile.

The MF Boogie Blues

The next number I choose from the select list of phone-phreak alumni, prepared for me by the blue-box inventor, is a Memphis number. It is the number of Joe Engressia, the first and still perhaps the most accomplished blind phone phreak.

Three years ago Engressia was a nine-day wonder in newspapers and magazines all over America because he had been discovered whistling free long-distance connections for fellow students at the University of South Florida. Engressia was born with perfect pitch: he could whistle phone tones better than the phone-company's equipment.

Engressia might have gone on whistling in the dark for a few friends for the rest of his life if the phone company hadn't decided to expose him. He was warned, disciplined by the college, and the whole case became public. In the months following media reports of his talent, Engressia began receiving strange calls. There were calls from a group of kids in Los Angeles who could do some very strange things with the quirky General Telephone and Electronics circuitry in L.A.

suburbs. There were calls from a group of mostly blind kids in --, California, who had been doing some interesting experiments with Cap'n Crunch whistles and test loops. There was a group in Seattle, a group in Cambridge, Massachusetts, a few from New York, a few scattered across the country. Some of them had already equipped themselves with cassette and electronic M-F devices. For some of these groups, it was the first time they knew of the others.

The exposure of Engressia was the catalyst that linked the separate phone-phreak centers together. They all called Engressia. They talked to him about what he was doing and what they were doing. And then he told them -- the scattered regional centers and lonely independent phone phreakers -- about each other, gave them each other's numbers to call, and within a year the scattered phone-phreak centers had grown into a nationwide underground.

Joe Engressia is only twenty-two years old now, but along the phone-phreak network he is "the old man," accorded by phone phreaks something of the reverence the phone company bestows on Alexander Graham Bell. He seldom needs to make calls anymore. The phone phreaks all call him and let him know what new tricks, new codes, new techniques they have learned. Every night he sits like a sightless spider in his little apartment receiving messages from every tendril of his web. It is almost a point of pride with Joe that they call him.

But when I reached him in his Memphis apartment that night, Joe Engressia was lonely, jumpy and upset.

"God, I'm glad somebody called. I don't know why tonight of all nights I don't get any calls. This guy around here got drunk again tonight and propositioned me again. I keep telling him we'll never see eye to eye on this subject, if you know what I mean. I try to make light of it, you know, but he doesn't get it. I can head him out there getting drunker and I don't know what he'll do next. It's just that I'm really all alone here, just moved to Memphis, it's the first time I'm living on my own, and I'd hate for it to all collapse now. But I won't go to bed with him. I'm just not very interested in sex and even if I can't see him I know he's ugly.

"Did you hear that? That's him banging a bottle against the wall outside. He's nice. Well forget about it. You're doing a story on phone phreaks? Listen to this. It's the MF Boogie Blues.

Sure enough, a jumpy version of Muskrat Ramble boogies its way over the line, each note one of those long-distance phone tones. The music stops. A huge roaring voice blasts the phone off my ear: "AND THE QUESTION IS ..." roars the voice, "CAN A BLIND PERSON HOOK UP AN AMPLIFIER ON HIS OWN?"

The roar ceases. A high-pitched operator-type voice replaces it. "This is Southern Braille Tel. & Tel. Have tone, will phone."

This is succeeded by a quick series of M-F tones, a swift "kachink" and a deep reassuring voice: "If you need home care, call the visiting-nurses association. First National time in Honolulu is 4:32 p.m."

Joe back in his Joe voice again: "Are we seeing eye to eye? 'Si, si,' said the blind Mexican. Ahem. Yes. Would you like to know the weather in Tokyo?"

This swift manic sequence of phone-phreak vaudeville stunts and blind-boy jokes manages to keep Joe's mind off his tormentor only as long as it lasts.

"The reason I'm in Memphis, the reason I have to depend on that homosexual guy, is that this is the first time I've been able to live on my own and make phone trips on my own. I've been banned from all central offices around home in Florida, they knew me too well, and at the University some of my fellow scholars were always harassing me because I was on the dorm pay phone all the time and making fun of me because of my fat ass, which of course I do have, it's my physical fatness program, but I don't like to hear it every day, and if I can't phone trip and I can't phone phreak, I can't imagine what I'd do, I've been devoting three quarters of my life to it.

"I moved to Memphis because I wanted to be on my own as well as because it has a Number 5 crossbar switching system and some interesting little independent phone-company districts nearby and so far they don't seem to know who I am so I can go on phone tripping, and for me phone tripping is just as important as phone phreaking."

Phone tripping, Joe explains, begins with calling up a central-office switch room. He tells the switchman in a polite earnest voice that he's a blind college student interested in telephones, and could he perhaps have a guided tour of the switching station? Each step of the tour Joe likes to touch and feel relays, caress switching circuits, switchboards, crossbar arrangements.

So when Joe Engressia phone phreaks he feels his way through the circuitry of the country garden of forking paths, he feels switches shift, relays shunt, crossbars swivel, tandems engage and disengage even as he hears -- with perfect pitch -- his M-F pulses make the entire Bell system dance to his tune.

Just one month ago Joe took all his savings out of his bank and left home, over the emotional protests of his mother. "I ran away from home almost," he likes to say. Joe found a small apartment house on Union Avenue and began making phone trips. He'd take a bus a hundred miles south in Mississippi to see some old-fashioned Bell equipment still in use in several states, which had been puzzling. He'd take a bus three hundred miles to Charlotte, North Carolina, to look at some brand-new experimental equipment. He hired a taxi to drive him twelve miles to a suburb to tour the office of a small phone company with some interesting idiosyncrasies in its routing system. He was having the time of his life, he said, the most freedom and pleasure he had known.

In that month he had done very little long-distance phone phreaking from his own phone. He had begun to apply for a job with the phone company, he told me, and he wanted to stay away from anything illegal.

"Any kind of job will do, anything as menial as the most lowly operator. That's probably all they'd give me because I'm blind. Even though I probably know more than most switchmen. But that's okay. I want to work for Ma Bell. I don't hate Ma Bell the way Gilbertson and some phone phreaks do. I don't want to screw Ma Bell. With me it's the pleasure of pure knowledge. There's something beautiful about the system when you know it intimately the way I do. But I don't know how much they know about me here. I have a very intuitive feel for the condition of the line I'm on, and I think they're monitoring me off and on lately, but I haven't been doing much illegal. I have to make a few calls to switchmen once in a while which aren't strictly legal, and once I took an acid trip and was having these auditory hallucinations as if I were trapped and these planes were dive-bombing me, and all of sudden I had to phone phreak out of there. For some reason I had to call Kansas City, but that's all."

A Warning Is Delivered

At this point -- one o'clock in my time zone -- a loud knock on my motel-room door interrupts our conversation. Outside the door I find a uniformed security guard who informs me that there has been an "emergency phone call" for me while I have been on the line and that the front desk has sent him up to let me know.

Two seconds after I say good-bye to Joe and hang up, the phone rings.

"Who were you talking to?" the agitated voice demands. The voice belongs to Captain Crunch. "I called because I decided to warn you of something. I decided to warn you to be careful. I don't want this information you get to get to the radical underground. I don't want it to get into the wrong hands. What would you say if I told you it's possible for three phone phreaks to saturate the phone system of the nation. Saturate it. Busy it out. All of it. I know how to do this. I'm not gonna tell. A friend of mine has already saturated the trunks between Seattle and New York. He did it with a computerized M-F-er hitched into a special Manitoba exchange. But there are other, easier ways to do it."

Just three people? I ask. How is that possible?

"Have you ever heard of the long-lines guard frequency? Do you know about stacking tandems with 17 and 2600? Well, I'd advise you to find out about it. I'm not gonna tell you. But whatever you do, don't let this get into the hands of the radical underground."

(Later Gilbertson, the inventor, confessed that while he had always been skeptical about the Captain's claim of the sabotage potential of trunk-tying phone phreaks, he had recently heard certain demonstrations which convinced him the Captain was not speaking idly. "I think it might take more than three people, depending on how many machines like Captain Crunch's were available. But even though the Captain sounds a little weird, he generally turns out to know what he's talking about.")

"You know," Captain Crunch continues in his admonitory tone, "you know the younger phone phreaks call Moscow all the time. Suppose everybody were to call Moscow. I'm no right-winger. But I value my life. I don't want the Commies coming over and dropping a bomb on my head. That's why I say you've got to be careful about who gets this information."

The Captain suddenly shifts into a diatribe against those phone phreaks who don't like the phone company.

"They don't understand, but Ma Bell knows everything they do. Ma Bell knows. Listen, is this line hot? I just heard someone tap in. I'm not paranoid, but I can detect things like that. Well, even if it is, they know that I know that they know that I have a bulk eraser. I'm very clean." The Captain pauses, evidently torn between wanting to prove to the phone-company monitors that he does nothing illegal, and the desire to impress Ma Bell with his prowess. "Ma Bell knows how good I am. And I am quite good. I can detect reversals, tandem switching, everything that goes on on a line. I have relative pitch now. Do you know what that means? My ears are a $20,000 piece of equipment. With my ears I can detect things they can't hear with their equipment. I've had employment problems. I've lost jobs. But I want to show Ma Bell how good I am. I don't want to screw her, I want to work for her. I want to do good for her. I want to help her get rid of her flaws and become perfect. That's my number-one goal in life now." The Captain concludes his warnings and tells me he has to be going. "I've got a little action lined up for tonight," he explains and hangs up.

Before I hang up for the night, I call Joe Engressia back. He reports that his tormentor has finally gone to sleep -- "He's not blind drunk, that's the way I get, ahem, yes; but you might say he's in a drunken stupor." I make a date to visit Joe in Memphis in two days.

A Phone Phreak Call Takes Care of Business

The next morning I attend a gathering of four phone phreaks in -- (a California suburb). The gathering takes place in a comfortable split-level home in an upper-middle-class subdivision. Heaped on the kitchen table are the portable cassette recorders, M-F cassettes, phone patches, and line ties of the four phone phreaks present. On the kitchen counter next to the telephone is a shoe-box-size blue box with thirteen large toggle switches for the tones. The parents of the host phone phreak, Ralph, who is blind, stay in the living room with their sighted children. They are not sure exactly what Ralph and his friends do with the phone or if it's strictly legal, but he is blind and they are pleased he has a hobby which keeps him busy.

The group has been working at reestablishing the historic "2111" conference, reopening some toll-free loops, and trying to discover the dimensions of what seem to be new initiatives against phone phreaks by phone-company security agents.

It is not long before I get a chance to see, to hear, Randy at work. Randy is known among the phone phreaks as perhaps the finest con man in the game. Randy is blind. He is pale, soft and pear-shaped, he wears baggy pants and a wrinkly nylon white sport shirt, pushes his head forward from hunched shoulders somewhat like a turtle inching out of its shell. His eyes wander, crossing and recrossing, and his forehead is somewhat pimply. He is only sixteen years old.

But when Randy starts speaking into a telephone mouthpiece his voice becomes so stunningly authoritative it is necessary to look again to convince yourself it comes from a chubby adolescent Randy. Imagine the voice of a crack oil-rig foreman, a tough, sharp, weather-beaten Marlboro man of forty. Imagine the voice of a brilliant performance-fund gunslinger explaining how he beats the Dow Jones by thirty percent. Then imagine a voice that could make those two sound like Stepin Fetchit. That is sixteen-year-old Randy's voice.

He is speaking to a switchman in Detroit. The phone company in Detroit had closed up two toll-free loop pairs for no apparent reason, although heavy use by phone phreaks all over the country may have been detected. Randy is telling the switchman how to open up the loop and make it free again:

"How are you, buddy. Yeah. I'm on the board in here in Tulsa, Oklahoma, and we've been trying to run some tests on your loop-arounds and we find'em busied out on both sides ... Yeah, we've been getting a 'BY' on them, what d'ya say, can you drop cards on 'em? Do you have 08 on your number group? Oh that's okay, we've had this trouble before, we may have to go after the circuit. Here lemme give 'em to you: your frame is 05, vertical group 03, horizontal 5, vertical file 3. Yeah, we'll hang on here ... Okay, found it? Good. Right, yeah, we'd like to clear that busy out. Right. All you have to do is look for your key on the mounting plate, it's in your miscellaneous trunk frame. Okay? Right. Now pull your key from NOR over the LCT. Yeah. I don't know why that happened, but we've been having trouble with that one. Okay. Thanks a lot fella. Be seein' ya."

Randy hangs up, reports that the switchman was a little inexperienced with the loop-around circuits on the miscellaneous trunk frame, but that the loop has been returned to its free-call status.

Delighted, phone phreak Ed returns the pair of numbers to the active-status column in his directory. Ed is a superb and painstaking researcher. With almost Talmudic thoroughness he will trace tendrils of hints through soft-wired mazes of intervening phone-company circuitry back through complex linkages of switching relays to find the location and identity of just one toll-free loop. He spends hours and hours, every day, doing this sort of thing. He has somehow compiled a directory of eight hundred "Band-six in-WATS numbers" located in over forty states. Band-six in-WATS numbers are the big 800 numbers -- the ones that can be dialed into free from anywhere in the country.

Ed the researcher, a nineteen-year-old engineering student, is also a superb technician. He put together his own working blue box from scratch at age seventeen. (He is sighted.) This evening after distributing the latest issue of his in-WATS directory (which has been typed into Braille for the blind phone phreaks), he announces he has made a major new breakthrough:

"I finally tested it and it works, perfectly. I've got this switching matrix which converts any touch-tone phone into an M-F-er."

The tones you hear in touch-tone phones are not the M-F tones that operate the long-distance switching system. Phone phreaks believe A.T.&T. had deliberately equipped touch tones with a different set of frequencies to avoid putting the six master M-F tones in the hands of every touch-tone owner. Ed's complex switching matrix puts the six master tones, in effect put a blue box, in the hands of every touch-tone owner.

Ed shows me pages of schematics, specifications and parts lists. "It's not easy to build, but everything here is in the Heathkit catalog."

Ed asks Ralph what progress he has made in his attempts to reestablish a long-term open conference line for phone phreaks. The last big conference -- the historic "2111" conference -- had been arranged through an unused Telex test-board trunk somewhere in the innards of a 4A switching machine in Vancouver, Canada. For months phone phreaks could M-F their way into Vancouver, beep out 604 (the Vancouver area code) and then beep out 2111 (the internal phone-company code for Telex testing), and find themselves at any time, day or night, on an open wire talking with an array of phone phreaks from coast to coast, operators from Bermuda, Tokyo and London who are phone-phreak sympathizers, and miscellaneous guests and technical experts. The conference was a massive exchange of information. Phone phreaks picked each other's brains clean, then developed new ways to pick the phone company's brains clean. Ralph gave M F Boogies concerts with his home-entertainment-type electric organ, Captain Crunch demonstrated his round-the-world prowess with his notorious computerized unit and dropped leering hints of the "action" he was getting with his girl friends. (The Captain lives out or pretends to live out several kinds of fantasies to the gossipy delight of the blind phone phreaks who urge him on to further triumphs on behalf of all of them.) The somewhat rowdy Northwest phone-phreak crowd let their bitter internal feud spill over into the peaceable conference line, escalating shortly into guerrilla warfare; Carl the East Coast international tone relations expert demonstrated newly opened direct M-F routes to central offices on the island of Bahrein in the Persian Gulf, introduced a new phone-phreak friend of his in Pretoria, and explained the technical operation of the new Oakland-to Vietnam linkages. (Many phone phreaks pick up spending money by M-F-ing calls from relatives to Vietnam G.I.'s, charging $5 for a whole hour of trans-Pacific conversation.)

Day and night the conference line was never dead. Blind phone phreaks all over the country, lonely and isolated in homes filled with active sighted brothers and sisters, or trapped with slow and unimaginative blind kids in straitjacket schools for the blind, knew that no matter how late it got they could dial up the conference and find instant electronic communion with two or three other blind kids awake over on the other side of America. Talking together on a phone hookup, the blind phone phreaks say, is not much different from being there together. Physically, there was nothing more than a two-inch-square wafer of titanium inside a vast machine on Vancouver Island. For the blind kids >there< meant an exhilarating feeling of being in touch, through a kind of skill and magic which was peculiarly their own.

Last April 1, however, the long Vancouver Conference was shut off. The phone phreaks knew it was coming. Vancouver was in the process of converting from a step-by-step system to a 4A machine and the 2111 Telex circuit was to be wiped out in the process. The phone phreaks learned the actual day on which the conference would be erased about a week ahead of time over the phone company's internal-news-and-shop-talk recording.

For the next frantic seven days every phone phreak in America was on and off the 2111 conference twenty-four hours a day. Phone phreaks who were just learning the game or didn't have M-F capability were boosted up to the conference by more experienced phreaks so they could get a glimpse of what it was like before it disappeared. Top phone phreaks searched distant area codes for new conference possibilities without success. Finally in the early morning of April 1, the end came.

"I could feel it coming a couple hours before midnight," Ralph remembers. "You could feel something going on in the lines. Some static began showing up, then some whistling wheezing sound. Then there were breaks. Some people got cut off and called right back in, but after a while some people were finding they were cut off and couldn't get back in at all. It was terrible. I lost it about one a.m., but managed to slip in again and stay on until the thing died ... I think it was about four in the morning. There were four of us still hanging on when the conference disappeared into nowhere for good. We all tried to M-F up to it again of course, but we got silent termination. There was nothing there."

The Legendary Mark Bernay Turns Out To Be "The Midnight Skulker"

Mark Bernay. I had come across that name before. It was on Gilbertson's select list of phone phreaks. The California phone phreaks had spoken of a mysterious Mark Bernay as perhaps the first and oldest phone phreak on the West Coast. And in fact almost every phone phreak in the West can trace his origins either directly to Mark Bernay or to a disciple of Mark Bernay.

It seems that five years ago this Mark Bernay (a pseudonym he chose for himself) began traveling up and down the West Coast pasting tiny stickers in phone books all along his way. The stickers read something like "Want to hear an interesting tape recording? Call these numbers." The numbers that followed were toll-free loop-around pairs. When one of the curious called one of the numbers he would hear a tape recording pre-hooked into the loop by Bernay which explained the use of loop-around pairs, gave the numbers of several more, and ended by telling the caller, "At six o'clock tonight this recording will stop and you and your friends can try it out. Have fun."

"I was disappointed by the response at first," Bernay told me, when I finally reached him at one of his many numbers and he had dispensed with the usual "I never do anything illegal" formalities which experienced phone phreaks open most conversations.

"I went all over the coast with these stickers not only on pay phones, but I'd throw them in front of high schools in the middle of the night, I'd leave them unobtrusively in candy stores, scatter them on main streets of small towns. At first hardly anyone bothered to try it out. I would listen in for hours and hours after six o'clock and no one came on. I couldn't figure out why people wouldn't be interested. Finally these two girls in Oregon tried it out and told all their friends and suddenly it began to spread."

Before his Johny Appleseed trip Bernay had already gathered a sizable group of early pre-blue-box phone phreaks together on loop-arounds in Los Angeles. Bernay does not claim credit for the original discovery of the loop-around numbers. He attributes the discovery to an eighteen-year-old reform school kid in Long Beach whose name he forgets and who, he says, "just disappeared one day." When Bernay himself discovered loop-arounds independently, from clues in his readings in old issues of the Automatic Electric Technical Journal, he found dozens of the reform-school kid's friends already using them. However, it was one of Bernay's disciples in Seattle that introduced phone phreaking to blind kids. The Seattle kid who learned about loops through Bernay's recording told a blind friend, the blind kid taught the secret to his friends at a winter camp for blind kids in Los Angeles. When the camp session was over these kids took the secret back to towns all over the West. This is how the original blind kids became phone phreaks. For them, for most phone phreaks in general, it was the discovery of the possibilities of loop-arounds which led them on to far more serious and sophisticated phone-phreak methods, and which gave them a medium for sharing their discoveries.

A year later a blind kid who moved back east brought the technique to a blind kids' summer camp in Vermont, which spread it along the East Coast. All from a Mark Bernay sticker.

Bernay, who is nearly thirty years old now, got his start when he was fifteen and his family moved into an L.A. suburb serviced by General Telephone and Electronics equipment. He became fascinated with the differences between Bell and G.T.&E. equipment. He learned he could make interesting things happen by carefully timed clicks with the disengage button. He learned to interpret subtle differences in the array of clicks, whirrs and kachinks he could hear on his lines. He learned he could shift himself around the switching relays of the L.A. area code in a not-too-predictable fashion by interspersing his own hook-switch clicks with the clicks within the line. (Independent phone companies -- there are nineteen hundred of them still left, most of them tiny island principalities in Ma Bell's vast empire -- have always been favorites with phone phreaks, first as learning tools, then as Archimedes platforms from which to manipulate the huge Bell system. A phone phreak in Bell territory will often M-F himself into an independent's switching system, with switching idiosyncrasies which can give him marvelous leverage over the Bell System.

"I have a real affection for Automatic Electric Equipment," Bernay told me. "There are a lot of things you can play with. Things break down in interesting ways."

Shortly after Bernay graduated from college (with a double major in chemistry and philosophy), he graduated from phreaking around with G.T.&E. to the Bell System itself, and made his legendary sticker-pasting journey north along the coast, settling finally in Northwest Pacific Bell territory. He discovered that if Bell does not break down as interestingly as G.T.&E., it nevertheless offers a lot of "things to play with."

Bernay learned to play with blue boxes. He established his own personal switchboard and phone-phreak research laboratory complex. He continued his phone-phreak evangelism with ongoing sticker campaigns. He set up two recording numbers, one with instructions for beginning phone phreaks, the other with latest news and technical developments (along with some advanced instruction) gathered from sources all over the country.

These days, Bernay told me, he had gone beyond phone-phreaking itself. "Lately I've been enjoying playing with computers more than playing with phones. My personal thing in computers is just like with phones, I guess -- the kick is in finding out how to beat the system, how to get at things I'm not supposed to know about, how to do things with the system that I'm not supposed to be able to do."

As a matter of fact, Bernay told me, he had just been fired from his computer-programming job for doing things he was not supposed to be able to do. he had been working with a huge time-sharing computer owned by a large corporation but shared by many others. Access to the computer was limited to those programmers and corporations that had been assigned certain passwords. And each password restricted its user to access to only the one section of the computer cordoned off from its own information storager. The password system prevented companies and individuals from stealing each other's information.

"I figured out how to write a program that would let me read everyone else's password," Bernay reports. "I began playing around with passwords. I began letting the people who used the computer know, in subtle ways, that I knew their passwords. I began dropping notes to the computer supervisors with hints that I knew what I know. I signed them 'The Midnight Skulker.' I kept getting cleverer and cleverer with my messages and devising ways of showing them what I could do. I'm sure they couldn't imagine I could do the things I was showing them. But they never responded to me. Every once in a while they'd change the passwords, but I found out how to discover what the new ones were, and I let them know. But they never responded directly to the Midnight Skulker. I even finally designed a program which they could use to prevent my program from finding out what it did. In effect I told them how to wipe me out, The Midnight Skulker. It was a very clever program. I started leaving clues about myself. I wanted them to try and use it and then try to come up with something to get around that and reappear again. But they wouldn't play. I wanted to get caught. I mean I didn't want to get caught personally, but I wanted them to notice me and admit that they noticed me. I wanted them to attempt to respond, maybe in some interesting way."

Finally the computer managers became concerned enough about the threat of information-stealing to respond. However, instead of using The Midnight Skulker's own elegant self-destruct program, they called in their security personnel, interrogated everyone, found an informer to identify Bernay as The Midnight Skulker, and fired him.

"At first the security people advised the company to hire me full-time to search out other flaws and discover other computer freaks. I might have liked that. But I probably would have turned into a double double agent rather than the double agent they wanted. I might have resurrected The Midnight Skulker and tried to catch myself. Who knows? Anyway, the higher-ups turned the whole idea down."

You Can Tap the F.B.I.'s Crime Control Computer in the Comfort of Your Own Home, Perhaps

Computer freaking may be the wave of the future. It suits the phone-phreak sensibility perfectly. Gilbertson, the blue-box inventor and a lifelong phone phreak, has also gone on from phone-phreaking to computer-freaking. Before he got into the blue-box business Gilbertson, who is a highly skilled programmer, devised programs for international currency arbitrage.

But he began playing with computers in earnest when he learned he could use his blue box in tandem with the computer terminal installed in his apartment by the instrumentation firm he worked for. The print-out terminal and keyboard was equipped with acoustical coupling, so that by coupling his little ivory Princess phone to the terminal and then coupling his blue box on that, he could M-F his way into other computers with complete anonymity, and without charge; program and re-program them at will; feed them false or misleading information; tap and steal from them. He explained to me that he taps computers by busying out all the lines, then going into a verification trunk, listening into the passwords and instructions one of the time sharers uses, and them M-F-ing in and imitating them. He believes it would not be impossible to creep into the F.B.I's crime control computer through a local police computer terminal and phreak around with the F.B.I.'s memory banks. He claims he has succeeded in re-programming a certain huge institutional computer in such a way that it has cordoned off an entire section of its circuitry for his personal use, and at the same time conceals that arrangement from anyone else's notice. I have been unable to verify this claim.

Like Captain Crunch, like Alexander Graham Bell (pseudonym of a disgruntled-looking East Coast engineer who claims to have invented the black box and now sells black and blue boxes to gamblers and radical heavies), like most phone phreaks, Gilbertson began his career trying to rip off pay phones as a teenager. Figure them out, then rip them off. Getting his dime back from the pay phone is the phone phreak's first thrilling rite of passage. After learning the usual eighteen different ways of getting his dime back, Gilbertson learned how to make master keys to coin-phone cash boxes, and get everyone else's dimes back. He stole some phone-company equipment and put together his own home switchboard with it. He learned to make a simple "bread-box" device, of the kind used by bookies in the Thirties (bookie gives a number to his betting clients; the phone with that number is installed in some widow lady's apartment, but is rigged to ring in the bookie's shop across town, cops trace big betting number and find nothing but the widow).

Not long after that afternoon in 1968 when, deep in the stacks of an engineering library, he came across a technical journal with the phone tone frequencies and rushed off to make his first blue box, not long after that Gilbertson abandoned a very promising career in physical chemistry and began selling blue boxes for $1,500 apiece.

"I had to leave physical chemistry. I just ran out of interesting things to learn," he told me one evening. We had been talking in the apartment of the man who served as the link between Gilbertson and the syndicate in arranging the big $300,000 blue-box deal which fell through because of legal trouble. There has been some smoking.

"No more interesting things to learn," he continues. "Physical chemistry turns out to be a sick subject when you take it to its highest level. I don't know. I don't think I could explain to you how it's sick. You have to be there. But you get, I don't know, a false feeling of omnipotence. I suppose it's like phone-phreaking that way. This huge thing is there. This whole system. And there are holes in it and you slip into them like Alice and you're pretending you're doing something you're actually not, or at least it's no longer you that's doing what you thought you were doing. It's all Lewis Carroll. Physical chemistry and phone-phreaking. That's why you have these phone-phreak pseudonyms like The Cheshire Cat, the Red King, and The Snark. But there's something about phone-phreaking that you don't find in physical chemistry." He looks up at me:

"Did you ever steal anything?"

"Well yes, I ... "

"Then you know! You know the rush you get. It's not just knowledge, like physical chemistry. It's forbidden knowledge. You know. You can learn about anything under the sun and be bored to death with it. But the idea that it's illegal. Look: you can be small and mobile and smart and you're ripping off somebody large and powerful and very dangerous."

People like Gilbertson and Alexander Graham Bell are always talking about ripping off the phone company and screwing Ma

Bell. But if they were shown a single button and told that by pushing it they could turn the entire circuitry of A.T.&T. into molten puddles, they probably wouldn't push it. The disgruntled-inventor phone phreak needs the phone system the way the lapsed Catholic needs the Church, the way Satan needs a God, the way The Midnight Skulker needed, more than anything else, response.

Later that evening Gilbertson finished telling me how delighted he was at the flood of blue boxes spreading throughout the country, how delighted he was to know that "this time they're really screwed." He suddenly shifted gears.

"Of course. I do have this love/hate thing about Ma Bell. In a way I almost like the phone company. I guess I'd be very sad if they were to disintegrate. In a way it's just that after having been so good they turn out to have these things wrong with them. It's those flaws that allow me to get in and mess with them, but I don't know. There's something about it that gets to you and makes you want to get to it, you know."

I ask him what happens when he runs out of interesting, forbidden things to learn about the phone system.

"I don't know, maybe I'd go to work for them for a while."

"In security even?"

"I'd do it, sure. I just as soon play -- I'd just as soon work on either side."

"Even figuring out how to trap phone phreaks? I said, recalling Mark Bernay's game."

"Yes, that might be interesting. Yes, I could figure out how to outwit the phone phreaks. Of course if I got too good at it, it might become boring again. Then I'd have to hope the phone phreaks got much better and outsmarted me for a while. That would move the quality of the game up one level. I might even have to help them out, you know, 'Well, kids, I wouldn't want this to get around but did you ever think of -- ?' I could keep it going at higher and higher levels forever."

The dealer speaks up for the first time. He has been staring at the soft blinking patterns of light and colors on the translucent tiled wall facing him. (Actually there are no patterns: the color and illumination of every tile is determined by a computerized random-number generator designed by Gilbertson which insures that there can be no meaning to any sequence of events in the tiles.)

"Those are nice games you're talking about," says the dealer to his friend. "But I wouldn't mind seeing them screwed. A telephone isn't private anymore. You can't say anything you really want to say on a telephone or you have to go through that paranoid bullshit. 'Is it cool to talk on the phone?' I mean, even if it is cool, if you have to ask 'Is it cool,' then it isn't cool. You know. 'Is it cool,' then it isn't cool. You know. Like those blind kids, people are going to start putting together their own private telephone companies if they want to really talk. And you know what else. You don't hear silences on the phone anymore. They've got this time-sharing thing on long-distance lines where you make a pause and they snip out that piece of time and use it to carry part of somebody else's conversation. Instead of a pause, where somebody's maybe breathing or sighing, you get this blank hole and you only start hearing again when someone says a word and even the beginning of the word is clipped off. Silences don't count -- you're paying for them, but they take them away from you. It's not cool to talk and you can't hear someone when they don't talk. What the hell good is the phone? I wouldn't mind seeing them totally screwed."

The Big Memphis Bust

Joe Engressia never wanted to screw Ma Bell. His dream had always been to work for her.

The day I visited Joe in his small apartment on Union Avenue in Memphis, he was upset about another setback in his application for a telephone job.

"They're stalling on it. I got a letter today telling me they'd have to postpone the interview I requested again. My landlord read it for me. They gave me some runaround about wanting papers on my rehabilitation status but I think there's something else going on."

When I switched on the 40-watt bulb in Joe's room -- he sometimes forgets when he has guests -- it looked as if there was enough telephone hardware to start a small phone company of his own.

There is one phone on top of his desk, one phone sitting in an open drawer beneath the desk top. Next to the desk-top phone is a cigar-box-size M-F device with big toggle switches, and next to that is some kind of switching and coupling device with jacks and alligator plugs hanging loose. Next to that is a Braille typewriter. On the floor next to the desk, lying upside down like a dead tortoise, is the half-gutted body of an old black standard phone. Across the room on a torn and dusty couch are two more phones, one of them a touch-tone model; two tape recorders; a heap of phone patches and cassettes, and a life-size toy telephone.

Our conversation is interrupted every ten minutes by phone phreaks from all over the country ringing Joe on just about every piece of equipment but the toy phone and the Braille typewriter. One fourteen-year-old blind kid from Connecticut calls up and tells Joe he's got a girl friend. He wants to talk to Joe about girl friends. Joe says they'll talk later in the evening when they can be alone on the line. Joe draws a deep breath, whistles him off the air with an earsplitting 2600-cycle whistle. Joe is pleased to get the calls but he looked worried and preoccupied that evening, his brow constantly furrowed over his dark wandering eyes. In addition to the phone-company stall, he has just learned that his apartment house is due to be demolished in sixty days for urban renewal. For all its shabbiness, the Union Avenue apartment house has been Joe's first home-of-his-own and he's worried that he may not find another before this one is demolished.

But what really bothers Joe is that switchmen haven't been listening to him. "I've been doing some checking on 800 numbers lately, and I've discovered that certain 800 numbers in New Hampshire couldn't be reached from Missouri and Kansas. Now it may sound like a small thing, but I don't like to see sloppy work; it makes me feel bad about the lines. So I've been calling up switching offices and reporting it, but they haven't corrected it. I called them up for the third time today and instead of checking they just got mad. Well, that gets me mad. I mean, I do try to help them. There's something about them I can't understand -- you want to help them and they just try to say you're defrauding them."

It is Sunday evening and Joe invites me to join him for dinner at a Holiday Inn. Frequently on Sunday evening Joe takes some of his welfare money, calls a cab, and treats himself to a steak dinner at one of Memphis' thirteen Holiday Inns. (Memphis is the headquarters of Holiday Inn. Holiday Inns have been a favorite for Joe ever since he made his first solo phone trip to a Bell switching office in Jacksonville, Florida, and stayed in the Holiday Inn there. He likes to stay at Holiday Inns, he explains, because they represent freedom to him and because the rooms are arranged the same all over the country so he knows that any Holiday Inn room is familiar territory to him. Just like any telephone.)

Over steaks in the Pinnacle Restaurant of the Holiday Inn Medical Center on Madison Avenue in Memphis, Joe tells me the highlights of his life as a phone phreak.

At age seven, Joe learned his first phone trick. A mean baby-sitter, tired of listening to little Joe play with the phone as he always did, constantly, put a lock on the phone dial. "I got so mad. When there's a phone sitting there and I can't use it ... so I started getting mad and banging the receiver up and down. I noticed I banged it once and it dialed one. Well, then I tried banging it twice ... " In a few minutes Joe learned how to dial by pressing the hook switch at the right time. "I was so excited I remember going 'whoo whoo' and beat a box down on the floor."

At age eight Joe learned about whistling. "I was listening to some intercept non working-number recording in L.A.- I was calling L.A. as far back as that, but I'd mainly dial non working numbers because there was no charge, and I'd listen to these recordings all day. Well, I was whistling 'cause listening to these recordings can be boring after a while even if they are from L.A., and all of a sudden, in the middle of whistling, the recording clicked off. I fiddled around whistling some more, and the same thing happened. So I called up the switch room and said, 'I'm Joe. I'm eight years old and I want to know why when I whistle this tune the line clicks off.' He tried to explain it to me, but it was a little too technical at the time. I went on learning. That was a thing nobody was going to stop me from doing. The phones were my life, and I was going to pay any price to keep on learning. I knew I could go to jail. But I had to do what I had to do to keep on learning."

The phone is ringing when we walk back into Joe's apartment on Union Avenue. It is Captain Crunch. The Captain has been following me around by phone, calling up everywhere I go with additional bits of advice and explanation for me and whatever phone phreak I happen to be visiting. This time the Captain reports he is calling from what he describes as "my hideaway high up in the Sierra Nevada." He pulses out lusty salvos of M-F and tells Joe he is about to "go out and get a little action tonight. Do some phreaking of another kind, if you know what I mean." Joe chuckles.

The Captain then tells me to make sure I understand that what he told me about tying up the nation's phone lines was true, but that he and the phone phreaks he knew never used the technique for sabotage. They only learned the technique to help the phone company.

"We do a lot of troubleshooting for them. Like this New Hampshire/Missouri WATS-line flaw I've been screaming about. We help them more than they know."

After we say good-bye to the Captain and Joe whistles him off the line, Joe tells me about a disturbing dream he had the night before: "I had been caught and they were taking me to a prison. It was a long trip. They were taking me to a prison a long long way away. And we stopped at a Holiday Inn and it was my last night ever using the phone and I was crying and crying, and the lady at the Holiday Inn said, 'Gosh, honey, you should never be sad at a Holiday Inn. You should always be happy here. Especially since it's your last night.' And that just made it worse and I was sobbing so much I couldn't stand it."

Two weeks after I left Joe Engressia's apartment, phone-company security agents and Memphis police broke into it. Armed with a warrant, which they left pinned to a wall, they confiscated every piece of equipment in the room, including his toy telephone. Joe was placed under arrest and taken to the city jail where he was forced to spend the night since he had no money and knew no one in Memphis to call.

It is not clear who told Joe what that night, but someone told him that the phone company had an open-and-shut case against him because of revelations of illegal activity he had made to a phone-company undercover agent.

By morning Joe had become convinced that the reporter from Esquire, with whom he had spoken two weeks ago, was the undercover agent. He probably had ugly thoughts about someone he couldn't see gaining his confidence, listening to him talk about his personal obsessions and dreams, while planning all the while to lock him up.

"I really thought he was a reporter," Engressia told the Memphis Press-Seminar. "I told him everything ... " Feeling betrayed, Joe proceeded to confess everything to the press and police.

As it turns out, the phone company did use an undercover agent to trap Joe, although it was not the Esquire reporter.

Ironically, security agents were alerted and began to compile a case against Joe because of one of his acts of love for the system: Joe had called an internal service department to report that he had located a group of defective long-distance trunks, and to complain again about the New Hampshire/Missouri WATS problem. Joe always liked Ma Bell's lines to be clean and responsive. A suspicious switchman reported Joe to the security agents who discovered that Joe had never had a long-distance call charged to his name.

Then the security agents learned that Joe was planning one of his phone trips to a local switching office. The security people planted one of their agents in the switching office. He posed as a student switchman and followed Joe around on a tour. He was extremely friendly and helpful to Joe, leading him around the office by the arm. When the tour was over he offered Joe a ride back to his apartment house. On the way he asked Joe -- one tech man to another -- about "those blue boxers" he'd heard about. Joe talked about them freely, talked about his blue box freely, and about all the other things he could do with the phones.

The next day the phone-company security agents slapped a monitoring tape on Joe's line, which eventually picked up an illegal call. Then they applied for the search warrant and broke in.

In court Joe pleaded not guilty to possession of a blue box and theft of service. A sympathetic judge reduced the charges to malicious mischief and found him guilty on that count, sentenced him to two thirty-day sentences to be served concurrently and then suspended the sentence on condition that Joe promise never to play with phones again. Joe promised, but the phone company refused to restore his service. For two weeks after the trial Joe could not be reached except through the pay phone at his apartment house, and the landlord screened all calls for him.

Phone-phreak Carl managed to get through to Joe after the trial, and reported that Joe sounded crushed by the whole affair.

"What I'm worried about," Carl told me, "is that Joe means it this time. The promise. That he'll never phone-phreak again. That's what he told me, that he's given up phone-phreaking for good. I mean his entire life. He says he knows they're going to be watching him so closely for the rest of his life he'll never be able to make a move without going straight to jail. He sounded very broken up by the whole experience of being in jail. It was awful to hear him talk that way. I don't know. I hope maybe he had to sound that way. Over the phone, you know."

He reports that the entire phone-phreak underground is up in arms over the phone company's treatment of Joe. "All the while Joe had his hopes pinned on his application for a phone-company job, they were stringing him along getting ready to bust him. That gets me mad. Joe spent most of his time helping them out. The bastards. They think they can use him as an example. All of sudden they're harassing us on the coast. Agents are jumping up on our lines. They just busted --'s mute yesterday and ripped out his lines. But no matter what Joe does, I don't think we're going to take this lying down."

Two weeks later my phone rings and about eight phone phreaks in succession say hello from about eight different places in the country, among them Carl, Ed, and Captain Crunch. A nationwide phone-phreak conference line has been reestablished through a switching machine in --, with the cooperation of a disgruntled switchman.

"We have a special guest with us today," Carl tells me.

The next voice I hear is Joe's. He reports happily that he has just moved to a place called Millington, Tennessee, fifteen miles outside of Memphis, where he has been hired as a telephone-set repairman by a small independent phone company. Someday he hopes to be an equipment troubleshooter.

"It's the kind of job I dreamed about. They found out about me from the publicity surrounding the trial. Maybe Ma Bell did me a favor busting me. I'll have telephones in my hands all day long."

"You know the expression, 'Don't get mad, get even'?" phone-phreak Carl asked me. "Well, I think they're going to be very sorry about what they did to Joe and what they're trying to do to us."

The History of ESS

Another original phile by
Lex Luthor

Of all the new 1960s wonders of telephone technology - satellites, ultra modern Traffic Service Positions (TSPS) for operators, the picturephone, and so on - the one that gave Bell Labs the most trouble, and unexpectedly became the greatest development effort in Bell System's history, was the perfection of an electronic switching system, or ESS.

It may be recalled that such a system was the specific end in view when the project that had culminated in the invention of the transistor had been launched back in the 1930s. After successful accomplishment of that planned miracle in 1947-48, further delays were brought about by financial stringency and the need for further development of the transistor itself. In the early 1950s, a Labs team began serious work on electronic switching. As early as 1955, Western Electric became involved when five engineers from the Hawthorne works were assigned to collaborate with the Labs on the project. The president of AT&T in 1956, wrote confidently, "At Bell Labs, development of the new electronic switching system is going full speed ahead. We are sure this will lead to many improvements in service and also to greater efficiency. The first service trial will start in Morris, Ill., in 1959." Shortly thereafter, Kappel said that the cost of the whole project would probably be $45 million.

But it gradually became apparent that the development of a commercially usable electronic switching system -in effect, a computerized telephone exchange - presented vastly greater technical problems than had been anticipated, and that, accordingly, Bell Labs had vastly underestimated both the time and the investment needed to do the job. The year 1959 passed without the promised first trial at Morris, Illinois; it was finally made in November 1960, and quickly showed how much more work remained to be done. As time dragged on and costs mounted, there was a concern at AT&T and some-thing approaching panic at Bell Labs. But the project had to go forward; by this time the investment was too great to be sacrificed, and in any case, forward projections of increased demand for telephone service indicated that within a phew years a time would come when, without the quantum leap in speed and flexibility that electronic switching would provide, the national network would be unable to meet the demand. In November 1963, an all-electronic switching system went into use at the Brown Engineering Company at Cocoa Beach, Florida. But this was a small installation, essentially another test installation, serving only a single company. Kappel's tone on the subject in the 1964 annual report was, for him, an almost apologetic: "Electronic switching equipment must be manufactured in volume to unprecedented standards of reliability.... To turn out the equipment economically and with good speed, mass production methods must be developed; but, at the same time, there can be no loss of precision..." Another year and millions of dollars later, on May 30, 1965, the first commercial electric central office was put into service at Succasunna, New Jersey.

Even at Succasunna, only 200 of the town's 4,300 subscribers initially had the benefit of electronic switching's added speed and additional services, such as provision for three party conversations and automatic transfer of incoming calls. But after that, ESS was on its way. In January 1966, the second commercial installation, this one serving 2,900 telephones, went into service in Chase, Maryland. By the end of 1967 there were additional ESS offices in California, Connecticut, Minnesota, Georgia, New York, Florida, and Pennsylvania; by the end of 1970 there were 120 offices serving 1.8 million customers; and by 1974 there were 475 offices serving 5.6 million customers.

The difference between conventional switching and electronic switching is the difference between "hardware" and "software"; in the former case, maintenance is done on the spot, with screwdriver and pliers, while in the case of electronic switching, it can be done remotely, by computer, from a central point, making it possible to have only one or two technicians on duty at a time at each switching center.

The development program, when the final figures were added up, was found to have required a staggering four thousand man-years of work at Bell Labs and to have cost not $45 million but $500 million!

The History of British Phreaking

Another original phile by

Note: The British Post Office, is the U.S. equivalent of Ma Bell.

In Britain, phreaking goes back to the early fifties, when the technique of 'toll a drop back' was discovered. Toll a was an exchange near st. Pauls which routed calls between london and nearby non-london exchanges. The trick was to dial an unallocated number, and then depress the receiver-rest for 1/2 second. This flashing initiated the 'clear forward' signal, leaving the caller with an open line into the toll a exchange.the could then dial 018, which forwarded him to the trunk exchange at that time, the first long distance exchange in britain and follow it with the code for the distant exchange to which he would be connected at no extra charge.

The signals needed to control the uk network today were published in the "institution of post office engineers journal" and reprinted in the sunday times (15 oct. 1972).

The signalling system they use: signalling system no. 3 Uses pairs of frequencies selected from 6 tones separated by 120Hz. With that info, the phreaks made "bleepers" or as they are called here in the u.s. "Blue box", but they do utilize different mf tones then the u.s., thus, your u.s. Blue box that you smuggled into the uk will not work, unless you change the frequencies.

In the early seventies, a simpler system based on different numbers of pulses with the same frequency (2280Hz) was used. For more info on that, try to get a hold of: Atkinson's "Telephony and Systems Technology".

In the early days of british phreaking, the Cambridge university titan computer was used to record and circulate numbers found by the exhaustive dialing of local networks. These numbers were used to create a chain of links from local exchange to local exchange across the country, bypassing the trunk circuits. Because the internal routing codes in the uk network are not the same as those dialed by the caller, the phreaks had to discover them by 'probe and listen' techniques or more commonly known in the u.s.-- scanning. What they did was put in likely signals and listened to find out if they succeeded. The results of scanning were circulated to other phreaks. Discovering each other took time at first, but eventually the phreaks became organized. The "tap" of britain was called "undercurrents" which enabled british phreaks to share the info on new numbers, equipment etc.

To understand what the british british phreaks did, think of the phone network in three layers of lines: local, trunk, and international.#in the uk, subscriber trunk dialing (std), is the mechanism which takes a call from the local lines and (legitimately) elevates it to a trunk or international level.#the uk phreaks figured that a call at trunk level can be routed through any number of exchanges, provided that the right routing codes were found and used correctly. They also had to discover how to get from local to trunk level either without being charged (which they did with a bleeper box) or without using (std). Chaining has already been mentioned but it requires long strings of digits and speech gets more and more faint as the chain grows, just like it does when you stack trunks back and forth across the u.s.#the way the security reps snagged the phreaks was to put a simple 'printermeter' or as we call it: a pen register on the suspects line, which shows every digit dialed from the subscribers line.

The British prefer to get onto the trunks rather than chaining. One way was to discover where local calls use the trunks between neighboring exchanges, start a call and stay on the trunk instead of returning to the local level on reaching the distant switch. This again required exhaustive dialing and made more work for titan; it also revealed 'fiddles', which were inserted by post office engineers.

What fiddling means is that the engineers rewired the exchanges for their own benefit. The equipment is modified to give access to a trunk with out being charged, an operation which is pretty easy in step by step (sxs) electromechanical exchanges, which were installed in britain even in the 1970s (note: I know of a back door into the canadian system on a 4a co., so if you are on sxs or a 4a, try scanning 3 digit exchanges, ie: dial 999,998,997 etc.#and listen for the beep-kerchink, if there are no 3 digit codes which allow direct access to a tandem in your local exchange and bypasses the ama so you won't be billed, not have to blast 2600 every time you wish to box a call.

A famous british 'fiddler' revealed in the early 1970s worked by dialing 173. The caller then added the trunk code of 1 and the subscribers local number. At that time, most engineering test services began with 17x, so the engineers could hide their fiddles in the nest of service wires. When security reps started searching, the fiddles were concealed by tones signalling: 'number unobtainalbe' or 'equipment engaged' which switched off after a delay. The necessary relays are small and easily hidden.

There was another side to phreaking in the uk in the sixties. Before std was widespread, many 'ordinary' people were driven to.

Occasional phreaking from sheer frustration at the inefficient operator controlled trunk system. This came to a head during a strike about 1961 when operators could not be reached. Nothing complicated was needed. Many operators had been in the habit of repeating the codes as they dialled the requested numbers so people soon learnt the numbers they called frequently. The only 'trick' was to know which exchanges could be dialled through to pass on the trunk number.callers also needed a pretty quiet place to do it, since timing relative to clicks was important the most famous trial of british phreaks was called the old baily trial.#which started on 3 oct. 1973.#What they phreaks did was to dial a spare number at a local call rate but involving a trunk to another exchange then they send a 'clear forward' to their local exchange, indicating to it that the call is finished;but the distant exchange doesn't realize because the caller's phone is still off the hook. They now have an open line into the distant trunk exchange and sends to it a 'seize' signal: '1' which puts him onto its outgoing lines now, if they know the codes, the world is open to them. All other exchanges trust his local exchange to handle the billing; they just interpret the tones they hear. Mean while, the local exchange collects only for a local call. The investigators discovered the phreaks holding a conference somewhere in england surrounded by various phone equipment and bleeper boxes, also printouts listing 'secret' post office codes. (They probably got them from trashing?) the judge said: "some take to heroin, some take to telephones" for them phone phreaking was not a crime but a hobby to be shared with phellow enthusiasts and discussed with the post office openly over dinner and by mail. Their approach and attitude to the worlds largest computer, the global telephone system, was that of scientists conducting experiments or programmers and engineers testing programs and systems. The judge appeared to agree, and even asked them for phreaking codes to use from his local exchange!

The End

Bad as Shit

Recently, a telephone fanatic in the northwest made an interesting discovery. He was exploring the 804 area code (Virginia) and found out that the 840 exchange did something strange.

In the vast majority of cases, in fact in all of the cases except one, he would get a recording as if the exchange didn't exist. However, if he dialed 804-840 and four rather predictable numbers, he got a ring!

After one or two rings, somebody picked up. Being experienced at this kind of thing, he could tell that the call didn't "supe", that is, no charges were being incurred for calling this number.

(Calls that get you to an error message, or a special operator, generally don't supervise.) A female voice, with a hint of a Southern accent said, "Operator, can I help you?"

"Yes," he said, "What number have I reached?"

"What number did you dial, sir?"

He made up a number that was similar.

"I'm sorry that is not the number you reached." Click.

He was fascinated. What in the world was this? He knew he was going to call back, but before he did, he tried some more experiments. He tried the 840 exchange in several other area codes. In some, it came up as a valid exchange. In others, exactly the same thing happened -- the same last four digits, the same Southern belle. Oddly enough, he later noticed, the areas worked in seemed to travel in a beeline from Washington DC to Pittsburgh, PA.

He called back from a payphone. "Operator, can I help you?"

"Yes, this is the phone company. I'm testing this line and we don't seem to have an identification on your circuit. What office is this, please?"

"What number are you trying to reach?"

"I'm not trying to reach any number. I'm trying to identify this circuit."

"I'm sorry, I can't help you."

"Ma'am, if I don't get an ID on this line, I'll have to disconnect it. We show no record of it here."

"Hold on a moment, sir."

After about a minute, she came back. "Sir, I can have someone speak to you. Would you give me your number, please?"

He had anticipated this and he had the payphone number ready. After he gave it, she said, "Mr. XXX will get right back to you."

"Thanks." He hung up the phone. It rang. INSTANTLY! "Oh my God," he thought, "They weren't asking for my number -- they were confirming it!"

"Hello," he said, trying to sound authoritative.

"This is Mr. XXX. Did you just make an inquiry to my office concerning a phone number?"

"Yes. I need an identi--"

"What you need is advice. Don't ever call that number again. Forget you ever knew it."

At this point our friend got so nervous he just hung up. He expected to hear the phone ring again but it didn't.

Over the next few days he racked his brains trying to figure out what the number was. He knew it was something big -- that was pretty certain at this point. It was so big that the number was programmed into every central office in the country. He knew this because if he tried to dial any other number in that exchange, he'd get a local error message from his CO, as if the exchange didn't exist.

It finally came to him. He had an uncle who worked in a federal agency. He had a feeling that this was government related and if it was, his uncle could probably find out what it was. He asked the next day and his uncle promised to look into the matter.

The next time he saw his uncle, he noticed a big change in his manner. He was trembling. "Where did you get that number?!" he shouted. "Do you know I almost got fired for asking about it?!? They kept wanting to know where I got it."

Our friend couldn't contain his excitement. "What is it?" he pleaded. "What's the number?!"

"IT'S THE PRESIDENT'S BOMB SHELTER!"

He never called the number after that. He knew that he could probably cause quite a bit of excitement by calling the number and saying something like, "The weather's not good in Washington. We're coming over for a visit." But our friend was smart. he knew that there were some things that were better off unsaid and undone. <>

<<> G-File: The Official Phreakers Manual: PHREAK*.DOC   93
G_PHREAK.WPS 11/20/90 11:29 AM

Chapter 3

This chapter is really just a bunch of FACS (pun intended). Here is where random facts that really have something to do with everything else but nothing to do with anything else, are presented. They cover various topics such as: Conferencing, Tracing, Pen registers, Calling cards, and some basic FMF (Fool the Mother Fuckers). The aspects covered here are very brief and could easily be covered much more thoroughly, but it is no problem since they are not very important topics. Something that would make a very nice gift is covered in the article AT&T forgery. Just make up stationary with AT&T letter head and give it as a present to your phriends who would appreciate it.

Phreaking COSMOS

COSMOS is Bell's computer for handling information on customer lines, special services on lines, and orders to change line equipment, disconnect lines, etc. COSMOS stands for Computerized System for Mainframe Operations. It is based on the UNIX operating system and, depending upon the COSMOS and upon your access, has some, many, or no UNIX standard commands. COSMOS is powerful, but there is no reason to be afraid of it. This article will give some of the basic, pertinent info on how users get in, account format, and a few other goodies.

Password Identification

To get onto COSMOS you need a dialup, account, password, and wire center (WC). Wire centers are two letter codes that tell what section of the COSMOS you are in. There are different WC's f or different areas and groups of exchanges. Examples are PB, SR, LK, et c. Sometimes there are accounts that have no password; obviously such accounts are the easiest to hack.

Checking It Out

Let's suppose you have a COSMOS number which you obtained one way or another. The first thing to do would be to make sure it is really a COSMOS system, not some other Bell or AT&T computer. To do this, you would call it and connect your modem,, then hit some returns until you got a response. It should say:

```
';LOGIN:' or 'NAME:'
```

If you enter some garbage it should say:

```
'PASSWORD:'
```

If you hit a return and it says 'WC?', it is a COSMOS system. If it says something like 'TA%' then you're in business. If it doesn't do any of the above, then it is either some other kind of system, or, if you're not getting anything at all, the dialup has probably gone bad.

Getting In

COSMOS has certain accounts that are usually on the system, one of which might not have a password. They consist of ROOT (most powerful and almost always on the system), SYS (second most powerful, still many privileges), BIN (a little less power), PREOP (a little less), and COSMOS (hardly any privileges, like a normal user). The way to tell if they have passwords is by entering accounts at the ';LOGIN:' or ' NAME:' prompt, and if it jumps straight to 'WC?', all you need is a WC to get in. But suppose all of the accounts have passwords? You have two choices. You can try to hack the password and WC to one of the above accounts. I won't deal with this method, as is self-explanatory. Or you can do something I find much easier...call the COSMOS during business hours and hope that someone forgot to log off. Keep calling until when you connect and hit return until you get a 'WC%' prompt. 'WC' is the WC that the account you found is currently in. You are now in!

What to Do While On-line

The first thing you want to do is write down the WC you are in. Only on our first login it is a good idea to print everything or dump everything to a buffer.

Commands

'WCFLDS'(!) Should list all WC's.

'WHO' Should print everyone currently logged on the system, giving some accounts.

'TTY' Tells what terminal port you are on.

'WHERE' Should tell the location of the COSMOS installation.

'WHAT' Tells what version of COSNIX, COSMOS's operating system, it is.

'LS *' Prints all the files you have access to.

'CD /dir' Connects you to the directory '/dir'.

'CAT filename ' Prints the file 'filename'.

'Q' Quits the editor.

CTRL-Y. Logs off

'TAT' Sometimes prints a little help file.

'ISH' Check someone's telefone #, type 'ISH' at the COSMOS 'WC%' prompt. Then type.

'HTN XXX-XXXX' (Hunt Telephone Number) to tell you about the local number you are interested in.

'CAT /ETC/PASSWD' Prints out the password file, if you have access. The passwords are almost always encrypted, but you get a list of all the accounts. If you are lucky, one of the lines will have two colons after the account name. This means there is no prompt from the ';LOGIN:' or 'NAME:' prompts when you enter that account.

To run a file just type the name followed by a return.

When the system gives you a '-', you type a '.', and it will type all kinds of info on the phone number you entered (in Bell abbreviations, of course). If it is not a good exchange, it will say something to that effect. You type a period to end the ISH.

If you wish to learn more information about COSMOS, find yourself a COSMOS manual or look at future issues of 2600. A UNIX manual would also be helpful for standard UNIX commands.

FACS Facts
A Look at the New FACS Systems

By Sharp Razor

Bell Atlantic (and probably the rest of the U.S. soon enough) is revamping Cosmos. The project is called FACS (facilitated assignment and control system).FACS is composed of 5 modules which are designed to function as a unified system. The PREMIS and the COSMOS systems can function as stand-alone systems.the five parts of FACS are PREMIS, SOAC, LFACS, COSMOS, and the wm.

The PREMIS (premises information system) supports both residence and business accounts. Premis is used for various inquiries for the street address guide(sag),ie::phone numbers,billing charges,credit,etc.

The second part of FACS is the SOAC(service order analysis and control). This is primarily used to input service order data into FACS, and to get the appropriate output. Soac interprets, validates,and decomposes all inputed data and sends the info to the COSMOS and the LFACS systems.

The third part of the system is LFACS (loop facilities and control system). This is the component of FACS that is responsible for maintaining the inventory,doing the assignments, administrating inquiries and reports, and is the inventory transformation center. This part of FACS will be mostly used for aiding the AT&T linemen.

The COSMOS system(computer system for mainframe operations) comprises the fourth part of the FACS system. Cosmos is the component of FACS that is responsible for maintaining the mechanized inventory of mdf facilities,storing custom call features(ie:speed dialing numbers),and other misc. Info.

The fifth and last piece of the FACS system is the work manager (wm). His component serves as the front-end processor for COSMOS. It enables a number of COSMOS computers to reliably communicate with the other FACS components. Wm serves as the messages switching system for the FACS pieces, and generally is the "messenger and stabilizer" of the system.

The hardware that will run this FACS system is:

COSMOS	22-weco. 3B-20s mini comps.
wm	6-weco. 3B-20s mini comps.
soac-lfacs-premis	two sperry univac 1100/92 mainframes. bancs 2 thp cyber 1000 processors.

The FACS system is starting up at this very moment. This is basically a broad view of the FACS system. At&t seems to think that FACS will be more efficient,save them money in the long run, and save them workers(here come some massive layoffs!) what this means to phreakers and hackers is that you will now have at least five dial-ups in an area code with which you can phuck with AT&T!

..later..
..sharp razor>>
..the legion of doom!

(Note: The FACS system has recently been put into operation(summer 84) in St.Louis Missouri)

Telenet

It seems that not many of you know that Telenet is connected to about 80 computer-networks in the world. No, I don't mean

80 nodes, but 80 networks with thousands of unprotected computers. When you call your local Telenet- gateway, you can only call those computers which accept reverse-charging-calls.

If you want to call computers in foreign countries or computers in USA which do not accept R-calls, you need a Telenet-ID. Did you ever notice that you can type ID XXXX when being connected to Telenet? You are then asked for the password. If you have such a NUI (Network-User-ID) you can call nearly every host connected to any computer-network in the world. Here are some examples:

026245400090184 Is a VAX in Germany (Username: DATEXP and leave mail for CHRIS !)

0311050500061 Is the Los Alamos Integrated computing network (One of the hosts connected to it is the DNA (Defense Nuclear Agency)!)

0530197000016 Is a BBS in New Zealand

024050256 Is the S-E-Bank in Stockholm, Sweden (Login as GAMES !)

02284681140541 CERN in Geneva in Switzerland (one of the biggest nuclear research centers in the world) Login as GUEST

0234212301161 A Videotex-standard system. Type OPTEL to get in and use the ID 999_ with the password 9_

0242211000001 University of Oslo in Norway (Type LOGIN 17,17 to play the Multi-User-Dungeon !)

0425130000215 Something like ITT Dialcom, but this one is in Israel ! ID HELP with password HELP works fine with security level 3

0310600584401 Is the Washington Post News Service via Tymnet (Yes, Tymnet is connected to Telenet, too !) ID and Password is: PETER

You can read the news of the next day !

The prefixes are as follows:

02624 is Datex-P in Germany
02342 is PSS in England
03110 is Telenet in USA
03106 is Tymnet in USA
02405 is Telepak in Sweden
04251 is Isranet in Israel
02080 is Transpac in France
02284 is Telepac in Switzerland
02724 is Eirpac in Ireland
02704 is Luxpac in Luxembourg
05252 is Telepac in Singapore
04408 is Venus-P in Japan

...and so on... Some of the countries have more than one packet-switching-network (USA has 11, Canada has 3, etc).

OK. That should be enough for the moment. As you see most of the passwords are very simple. This is because they must not have any fear of hackers. Only a few German hackers use these networks. Most of the computers are absolutely easy to hack ! So, try to find out some Telenet-ID's and leave them here. If you need more numbers, leave e-mail.

I'm calling from Germany via the German Datex-P network, which is similar to Telenet. We have a lot of those NUI's for the German network, but none for a special Tymnet-outdial-computer in USA, which connects me to any phone #.

CUL8R, Mad Max

ps. Call 026245621040000 and type ID INF300 with password DATACOM to get more information on packet-switching-networks !

ps. The new password for the Washington Post is KING !

Phreaking AT&T Cards

My topic will deal with using an AT&T calling card for automated calls. Ok to place a call with an AT&T card, lift the handset (PAY PHONE) hit (0) and the desired area code and the number to call. Also when calling the same number that the card is being billed to you enter the phone number and at the tone only enter the last four digits on the card. But we don't want to do that now, do we. If additional calls are wanted all you do is hit the (#) and you will get a new dial tone! After you hit (#) you do not have to re-enter the calling card number simply enter your desired number and it will connect you.

If the number you called is busy just keep hitting (#) and the number to be called until you connect! Ok to calL the U.S. of a from another country, you use the exact same format as described above!

Ok now I will describe the procedure for placing calls to a foreign country, such as CANADA,RUSSIA,SOUTH AMERICA, etc.. Ok first lift the handset then enter (01) + the country code + the city code + the local telephone number. Ok after you get the tone enter the AT&T calling card number. Ok if you can not dial operator assisted calls from your area don't worry just jingle the operator and she will handle your call, don't worry she can't see you!

The international number on the AT&T calling card is used for calling the US of A from places like RUSSIA, CHINA you never know when you might get stuck in a country like those and you have no money to make a call! The international operator will be able to tell you if they honor the AT&T calling card.

Well I hope that this has straightened out some of your problems on the use of an AT&T calling card! All you have to remember is that weather you are placing the call or the operator, be careful and never use the calling card from your home phone! That is a BIG NO NO..

Also AT&T has came out with a new thing called (NEW CARD CALLER SERVICE) they say that it was designed to meet the public's needs! These phones will be popping up in many place such as airport terminals, hotels, etc... What the new card caller service is, is a new type of phone that has a (CRT) screen that will talk to you in a language of your choice. The service works something like this, when you find a (NEW CARD CALLER PHONE), all you do is follow the instructions on the (CRT) screen, then you insert the (NEW CARD CALLER CARD) and there is a strip of magnetic tape on the card which reads the number, thus no one can hear you saying your number or if there were a bug in the phone,no touch tones will be heard! You can also bill the call to a third party. that is one that I am not totally clear on yet! The phone is supposed to tell you how it can be done. That is after you have inserted your card and lifted the receiver!

AT&T Forgery

Written by The Blue Buccaneer
Uploaded by Elric of Imrryr of Lunatic Labs UnLtd

Call the Everlasting Speed Demon BBS
(415) 522-3074

Here is a very simple way to either:

1. Play an incredibly cruel and realistic joke on a phreaking friend.

2. Provide yourself with everything you ever wanted to be an AT&T person.

All you need to do is get your hands on some AT&T paper and/or business cards. To do this you can either go down to your local business office and swipe a few or call up somewhere like WATTS INFORMATION and ask them to send you their information package. They will send you:

1. A nice letter (with the AT&T logo letterhead) saying "Here is the info."

2. A business card (again with AT&T) saying who the sales representative is.

3. A very nice color booklet telling you all about WATTS lines.

4. Various billing information. (Discard as it is very worthless)

Now take the piece of AT&T paper and the AT&T business card down to your local print/copy shop. Tell them to run you off several copies of each, but to leave out whatever else is printed on the business card/letter. If they refuse or ask why, take your precious business elsewhere. (This should only cost you around $2.00 total)

Now take the co ies home and either with your ty ewriter, MAC, or Fontrix, add whatever name, address, tele hone number, etc. you like. (I would recommend just changing the name on the card and using whatever information was on there earlier)

And there you have official AT&T letters and business cards. As mentioned earlier, you can use them in several ways. Mail a nice letter to someone you hate (on AT&T paper..hehehe) saying that AT&T is onto them or something like that. (Be sure to use correct English and spelling) (Also do not hand write the letter! Use a typewriter! - Not Fontrix as AT&T doesn't use OLD ENGLISH or ASCII BOLD when they type letters. Any IBM typewriter will do perfectly)

Another possible use (of many, I guess) is (if you are old enough to look the part) to use the business card as some sort of fake id.

The last example of uses for the fake AT&T letters & b.cards is mentioned in my textfile, BASIC RADIO CALLING. Briefly, send the station a letter that reads:

WCAT - FM202: (Like my examples? Haha!)

As you probably know, radio stations give away things by accepting the 'x' call. (ie: The tenth caller through wins a pair of Van Halen tickets) Sometimes they may ask a trivia question, but that's your problem. Anyway, the letter continues:

(You basically say that they have become so popular that they are getting too many calls at once from listeners trying to win tickets. By asking them to call all at the same time is overloading our systems. We do, of course, have means of handling these sort of matters, but it would require you sending us a schedule of when you will be asking your listeners to call in. That way we would be able to set our systems to handle the amount of callers you get at peak times..(etc..etc..more BS..But you get the idea, right?)

Joseph Hakimout
AT&T Telecommunications
East Bumblefuck, Nowheresville 55555

Ok, so it probably won't work (DJs just aren't that dumb, unless you really do live in Nowheresville), but using AT&T paper and a business card might up your chances some.

A Little Something About Your Phone Company

By Col. Hogan

Ever get an operator who gave you a hard time, and you didn't know what to do? Well if the operator hears you use a little Bell jargon, she might wise up. Here is a little diagram (excuse the artwork) of the structure of operators:

```
    +--------+      +------+      +-----+
    |Operator| ---> | S.A. | ---> | BOS |
    +--------+      +------+      +-----+
         |
         |
         V
 +-------------+
 | Group Chief |
 +-------------+
```

Now most of the operators are not bugged, so they can curse at you, if they do ask INSTANTLY for the "S.A." or the Service Assistant. The operator does not report to her (95% of them are hers) but they will solve most of your problems. She MUST give you her name as she connects & all of these calls are bugged. If the SA gives you a rough time get her BOS (Business Office Supervisor) on the line. S/He will almost always back her girls up, but sometimes the SA will get tarred and feathered. The operator reports to the Group Chief, and S/He will solve 100% of your problems, but the chances of getting S/He on the line are nill.

If a lineman (the guy who works out on the poles) or an installation man gives you the works ask to speak to the Installation Foreman, that works wonders.

Here is some other Bell jargon, that might come in handy if you are having trouble with the line. Or they can be used to lie your way out of situations....

An Erling is a line busy for 1 hour, used mostly in traffic studies A Permanent Signal is that terrible howling you get if you disconnect, but don't hang up.

Everyone knows what a busy signal is, but some idiots think that is the *Actual* ringing of the phone, when it just is a tone "beeps" when the phone is ringing, wouldn't bet on this though, it can (and does) get out of sync.

When you get a busy signal that is 2 times as fast as the normal one, the person you are trying to reach isn't really on the phone, (he might be), it is actually the signal that a trunk line somewhere is busy and they haven't or can't reroute your call. Sometimes you will get a Recording, or if you get nothing at all (Left High & Dry in fone terms) all the recordings are being used and the system is really overused, will probably go down in a little while. This happened when Kennedy was shot, the system just couldn't handle the calls. By the way this is called the "reorder signal" and the trunk line is "blocked".

One more thing, if an overseas call isn't completed and doesn't generate any money for AT&T, is is called an "Air & Water Call".

Essence of Telephone Conferencing

Written by Forest Ranger

Telephone conferencing is an easy way of getting many friends together at once. This can be accomplished easily with little or no trouble what so ever. The techniques that I will teach you do not require a blue box or a touch tone phone line. The only prerequisite is that you have a phone that has a tone switch on it or have a hookable touch tone keypad. Now, if you are the paranoid type of person and refuse to use your own phone out of your house then here are some simple ways of getting conferences started from another phone. Go to a mall or a place where you know the phone is being payed for by the business it is in.

Now there are two to call the conference operator; dial "0" to get your local operator so she can put you through to the conference operator or dial the conference operator directly if you have the number handy. The system you will be linked up to is called the "alliance" system. There are three branches; 1000,2000,3000.

Now once you have gotten the conference operator you tell her you would like to start a conference and you would like to maintain control of it. She will then proceed to ask you for your name and number. You will then give her a fake name and the number of the pay phone. She will hang up and call you back once she has checked the number. They usually don't realize it is a payphone so don't think it won't work! Now once the operator has given you control you will then proceed to hack my voice phone and put me on the conference.

Now, the other way of starting a conference in which you don't get a live operator is a "pbx". With this you will call a pbx number and you will then receive a recording of a business or office co. Then when the recording is over you will here a beep...then after about 10-30 seconds after the beep you will get a dial tone on the on the end of the pbx. You will then type the pbx code which will then respond with a recording welcoming you to the conferencing network (which will in most if not all be the "alliance" system).

It will be self explanatory from there. Now if you don't wish to call the conference operator either way already explained then there is a was of getting your friends in conference. This is done over a loop extension. No one will have control, but you will still be on conference. This is called the seven line loop extension. This means you can have up to seven members, but that is it! The number is in la, ca. 213-206-2820. The last way I will explain to you if you are in desperate need of a conference is to go to pay phone like I mentioned before any make sure some business pays the bill for it then call the conference operator in the fashions mentioned and ask the conference operator to place conference calls.

They will then ask for the numbers of the people to put on conference, you give her the numbers and she will put you all on conference. When you are done you will hang up on her so there will be no one in control.that means the conference will be billed to the payphone and no one can be blamed for the conference due to no one being in control! *Note* the conference operator will not be on while you are all talking! Remember that conferences are not hard and it is very hard to get arrested on one due to what I have mentioned.

Remember: Reach out and phreak someone!

Telephone Conference Controls

# -	control mode
# - 6	passes control
# - 1 + area code & number	adds
# - 9	silent mode
# - 7	gets conference operator
*	ends conference

The "#" is the control key on your conferences. When you pass control to someone else hit the "#" then "6". Wait for the recording to say enter # of person to pass control to, then enter the number of the person you are going to give control to.

To add a person on to the conference hit "#" then "1","area code","number". Then when the person answers wait five seconds then hit the "#" to add. If you are in control of the conference and you want to hear everyone else, but you do not want to be heard it "#" then "9" then the "#" to rejoin the conference. Remember after adding someone on or passing control to someone you must always hit the "#" to rejoin the others on conference: passing control: "#","6", wait for recording to say enter number of party to give control to then enter number and hit "#" to rejoin your conference.if you ever want to get a conference operator for some strange reason then hit "#","7" and wait for a conference operator to click on. To end a conference hit "*".

With help from: Silicon Falcon, Silver Condor, and the

Eliminator.

Phone Tapping

Here is some info on phone taps. I have enclosed a schematic for a simple wiretap & instructions for hooking up a tape recorder control relay to the phone line.

First I'll discuss taps a little. There are many different types of taps. There are transmitters, wired taps and induction taps to name a few. Wired and wireless transmitters must be physically connected to the line before they'll do any good. Once a wireless tap is connected to the line, it can transmit all conversations over a limited range. The phones in the house can even be modified to pick up conversations in the room & transmit them too! These taps are usually powered off the phone line, but can have an external power source.

Wired taps, on the other hand, need no power source, but a wire must be run from the line to the listener or to a transmitter. There are obvious advantages of wireless taps over wired ones. There is one type of wireless tap that looks like a normal telephone mike. All you have to do is replace the original mike with this & it'll transmit all conversations!

There is an exotic type of wired tap known as the 'infinity transmitter' or 'harmonica bug'. In order to hook up one of these, you need access to the target telephone. It has a tone decoder & switch inside. When it is installed, someone calls the tapped phone & *before* it rings, blows a whistle over the line. The x-mitter receives the tone & picks up the phone via a relay. The mike on the phone is activated so the caller can hear all conversations in the room.

There is a sweep tone test at 415/bug-1111 which can be used to detect on of these taps. If one of these is on your line & the test # sends the correct tone, you'll hear a click.

Induction taps have one big advantage over taps that must be physically wired to the phone. They don't have to be touching the phone in order to pick up the conversation. They work on the same principle as the little suction-cup tape recorder mikes you can get at radio shack. Induction mikes can be hooked up to a transmitter or be wired. Here is an example of industrial espionage using the phone:

A salesman walks into an office & makes a fone call. He fakes the conversation, but when he hangs up he slips some foam-rubber cubes under the handset, so the fone is still off the hook. The called party can still hear all conversations in the room. When someone picks up the fone, the cubes fall away unnoticed.

I use a tap on my line to monitor what ae-pro is doing when it auto-dials, since it doesn't take advantage of the handset on the apple cat II. I can also hook up the tap to a cassette recorder or amplifier. Here is the schematic:

```
     -------)!----)!(------------->
                  )!(
      cap ^       )!(
                  )!(
                  )!(
                  )!(
          ^^^^^---)!(------------->
            ^  100k
            !
            !<input
```

The 100k pot is used for volume. It should be on its highest (least resistance) setting if you hook a speaker across the output, but it should be set on its highest resistance for a tape recorder or amplifier. You may find it necessary to add another 10-40k. The capacitor should be around .47 mfd. It's only purpose is to prevent the relay in the co from tripping & thinking you have the fone off the hook. The audio output transformer available at radio shack (273-1380) is fine for the x-former. The black & green are fine for input & the red & white go to the output device. You may want to experiment with the x-former for the best output.

Hooking up a tape recorder control relay is east. Just one of the fone wires (usu. Red) before the telephones & hook one end to one wire of the relay & the other end to the other relay wire. Like this:

```
     ------^^^^^^^^^------------
           ---------
           relay^^
```

Wiretapping and Divestiture:
A Lineman Speaks Out

By the Knights of Shadow
2600 - January 1985

Never missing an opportunity for social engineering, the kid & co. And I naturally carried on a conversation with the new jersey Bell fone installer when he came to put in my modem line. The conversation turned to fone tapping, and several interesting details came to light. He swore up and down that Bell had nothing to do with wire tapping. He said the supervisor receives sealed orders from the sheriff's office, merely passing them on to the linemen. Then the linemen follow the orders to go up on the poles and mark the pair in the "can" that fit the fone line in question, and then leave the site.

One day, our lineman drove back by the pole he had marked earlier in the day, and saw a Bell truck. Wondering who it was, he stopped to ask. The guy up on the pole told him to go away and to leave him alone. Since our friendly lineman didn't recognize the mystery man as one of the linemen for the area, he asked his supervisor who it could have been. His supervisor curtly told him to forget the entire incident.

The lineman told us that in the old days the telco and the prosecutor's office worked hand-in-hand. They would let the authorities right into the co to listen in on conversations. But this ended around 1973 when someone sued jersey Bell because of this too close interaction. The telco then realized that they didn't have to go that far in order to help the police. After this they gradually broke from the close relationship. Now the fone company merely marks the lines, and the prosecutor's office handles the rest. He also said that now the police sometimes use ultrasonic waves bounced off of window panes to listen to suspects, removing all contact with the fone lines. Since the presence of a fone company truck messing with telephone wires is taken for granted by the general populace, the sheriff's office also has a couple of them for undercover work. Since they got them back in the good old days of Bell friendliness, the trucks tend to be the older models, with outdated gear. The lineman told us a sure way to identify the local police's trucks: they have wooden ladders. New jersey Bell switched over to plastic ones years ago.

Continuing the discussion with the lineman, we covered the breakup. New jersey Bell now no longer gives as much overtime as it once did. The lineman complained that his standard of living had gone down since the breakup as he no longer has as much take home pay. The breakup has caused a total severing of ties with AT&T. He professed total ignorance about long distance calling. He had originally gone with AT&T, but disliked fixing pbx's and computer systems. As soon as he could, he switched back to the local operating company.

He told us about a technical institute western union was operating somewhere in the midwest. He had gone there to learn about the various types of switching systems. On campus was a gigantic, multi-story building split up into rooms approximately the size of gymnasiums. In each was a fully operational scale model of each of the various switching systems. Western electric manufactures, including all the ESS and crossbar machines, as well as some step-by-step, and several types of pbx's. They trouble-shot and repaired problems in these machines in order to learn about actual operating equipment.

We talked about the local switching equipment, which turned out to be a #1a ESS. According to him, soon all the local co's will be run automatically from central locations called "hubs". The "hub" handles any overload between central offices that might cause the dreaded "gridlock" of the fone system. If the interoffice signaling lines get overloaded, the calls are rerouted through the hub. The hub also serves as a central spot where troubles at the local co are handled in the first stages of trouble-shooting. The "hub" concept is alive and well in our local area, with #5 ESS, the third installed in the entire nation, running the whole operation.

When he was getting ready to leave he thanked us for the interesting conversation, and we waved at him as he pulled out. I now not only had a new fone line, but also a lot of useful and interesting info, as well as the satisfaction of a friendly chat.

The lesson is clear. Whenever a Bell employee visits your house, fell phree to ask whatever you want, within reason. Most are extremely willing to shoot the bull about almost anything of which they have knowledge. At first, merely joke with them lightheartedly, in order to get them off there guard. Legit questions askable by a normal customer, such as equal access cutovers, will get them rolling, leaving you to direct the conversation wherever you like. Asking about the breakup and how it affected them is a sure fire way to get them talking. Questions like "how does the fone network work?" also are good, especially if you guide them into the discussion of switching technology. Most Bell employees are really glad to talk to someone. Remember, they usually interact with disgruntled customers with complaints. Their spouses probably yell at them, and their supervisors either complain about their performance or ignore them. Society at large just doesn't care about them. They're most probably disenchanted with the world at large, and maybe even dissatisfied with their jobs. The chance to talk to some one who merely wants to listen to what they say is a welcome change. They will talk on and on about almost anything, from telecommunications to their home life and their childhood. The possibilities for social engineering are endless. Remember, Bell employees are humans, too. All you have to do is listen.

PEN Registering and Tracing

Written by Forest Ranger

PEN registering is a special device used by AT&T. This device deciphers the tones used when phreaking phone calls. This means that each tone key pressed is deciphered if you had a PEN register on your line or were being traced with a PEN register, every phone number you dialed would be known. That means every time you would phreak a number not only would the access number be recorded, but the code being used and where you called to! So if you know you have a PEN register on your line then I would advise you not to phreak!

Tracing - the FBI does not trace,the police do not trace. The phone co. Traces. If the FBI wants a trace on your line they simply call the phone co. The FBI does not sit up all night to listen in on your phone. They don't trace for years or 6 months, but just for a few days at a time if at all. The police traces the same way. It costs too much money to trace all the computer phreakers and hackers, so they merely pick on a select few. So tracing isn't as dangerous as it seems! The people that tell you different have been watching too many late night films! So don't get too paranoid if you think you are being traced due to the facts mentioned above!

Forest Ranger

The Phone Phreak's Fry-Um Guide
Volume One, Issue One, Phile #4 of 8

Compiled by the Iron Soldier
With help from Dr. Dove

Note This guide is still being compiled, and as phone phreaks learn more in the art of vengeance it will always expand.

"Vengeance is mine", says the Phreak.

Method 1
Phone Line Phun

Call up the business office. It should be listed at the front of the white pages. Say you wanted to disconnect Scott Korman's line. DIAL 800-xxx-xxxx.

> "Hello, this is Mr. Korman, I'm moving to California and would like to have my phone service disconnected. I'm at the airport now. I'm calling from a payphone, my number is [414] 445 5005. You can send my final bill to: (somewhere in California). Thank you."

Method 2

Phone Books

Call up the business office from a pay phone. Say :

> "Hello, I'd like to order a Phone Book for Upper Volta (or any out-of-the way area with Direct Dialing). This is Scott Korman, ship to 3119 N. 44th St. Milwaukee, WI 53216. Yes, I under stand it will cost $xx($25-$75!). Thank you."

Method 3
Phone Calls

Call up a PBX, enter the code and get an outside line. Then dial 0+ the number desired to call. You will hear a bonk and then an operator. Say, "I'd like to charge this to my home phone at 414-445-5005. Thank you." A friend and I did this to a loser, I called him at 1:00 AM and we left the fone off the hook all night. I calculated that it cost him $168.

Method 4
Misc. Services

Call up the business office once again from a payfone. Say you'd like call waiting, forwarding, 3 way, etc. Once again you are the famed loser Scott Korman. He pays-you laugh. You don't know how funny it was talking to him, and wondering what those clicks he kept hearing were.

Method 5
Changed & Unpublished

Do the same as in #4, but say you'd like to change and unlist your (Scott's) number. Anyone calling him will get:

> "BEW BEW BEEP. The number you have reached, 445-5005, has been changed to a non-published number. No further....."

Method 6
Forwarding

This required an accomplice or two or three. Around Christmas time, go to Toys 'R' Us. Get everyone at the customer service or manager's desk away ("Hey, could you help me"). then you get on their phone and dial (usually dial 9 first) and the business office again. This time, say you are from Toys 'R' Us, and you'd like to add call forwarding to 445-5005. Scott will get 100-600 calls a day!

Method 7
Russian Caller

Call a payphone at 10:00 PM. Say to the operator that you'd like to book a call to Russia. Say you are calling from a payphone, and your number is that of the loser to fry (e.g. 445-5005). She will say that she'll have to call ya back in 5 hours, and you ok that. Meanwhile the loser (e.g.) Scott, will get a call at 3:00 AM from an operator saying that the call he booked to Russia is ready.

If you have any questions, leave e-mail for me on any board I'm on.

The Iron Soldier
TSF-The Second Foundation!

Interesting Things to do on Step Lines

---

if you have step lines in your prefix, (a good way of checking to see if you have step is to look at the payphones around your house, if they are rotary, then you have step, if not, your outta luck.)

From your house dial "0", (this will not work at a payphone). You will hear a few "kerplunks", if you hit the hang up button when the second-to-the-last "kerplunk" is heard then the operator will get on and be very confused. (I will tell why she is confused in just a second, but for now just....) say that you are trying to complete a call when she got on. She will ask for the number you are trying to call. Tell her the number (long distance of course), and she will ask you for your number, pick a number out of your head, (it must be in your prefix though), and tell her it. She will believe you and will connect you with the charges charged to the number you said. (If you didn't hit the button at the correct time just tell the operator your sorry, you were trying to dust the phone or some other bullshit like that.)

What you did was screw up the automatic number find that was built into the first step lines. This is what would tell the operator your number so she could bill you if she had to complete a call for you. The operator will get some garbage on her screen that is supposed to be your number, but since you interrupted that process, it looks really bizzare.

What is really phun to do is complain to the operator that this is the third time today that you have not been able to get through and she will give you some sob story about "we're sorry, but we've had a computer malfunction and it is being fixed right now".

I'm kinda sure that the phone company knows nothing of this. The worst thing that could happen is you get a call asking why you've hung up on the operator so many times, (if you did this alot, that is). Just give them some bullshit about a baby brother just learning how to use the phone, or something like that.

Live long and don't get caught,

Agrajag

Brought to you by Agrajag and the Hitchhikers

Bring your towel.

2600 Magazine's Story on the Private Sector Bust

Uploaded by Elric of Imrryr
Lunatic Labs Unlimited
Typed By Shooting Shark

The following article appeared in the August, 1985 issue of 2600 Magazine. Subscriptions to 2600 are $12 a year for individuals. Make checks payable to 2600 Enterprises, Inc. Write to: 2600, Box 752, Middle Island, NY 11953-0752. Their phone number is 516-751-2600. Text of article follows.

Seized!
2600 Bulletin Board is Implicated in Raid on Jersey Hackers

On July 12, 1985, law enforcement officials seized the Private Sector BBS, the official computer bulletin board of 2600 magazine, for "complicity in computer theft," under the newly passed, and yet untested, New Jersey Statute 2C:20-25. Police had uncovered in April a credit carding ring operated around a Middlesex County electronic bulletin board, and from there investigated other North Jersey bulletin boards. Not understanding subject matter of the Private Sector BBS, police assumed that the sysop was involved in illegal activities. Six other computers were also seized in this investigation, including those of Store Manager [perhaps they mean Swap Shop Manager? - Shark] who ran a BBS of his own, Beowolf, Red

Barchetta, the Vampire, NJ Hack Shack, sysop of the NJ Hack Shack BBS, and that of the sysop of the Treasure Chest BBS.

Immediately after this action, members of 2600 contacted the media, who were completely unaware of any of the raids. They began to bombard the Middlesex County Prosecutor's Office with questions and a press conference was announced for July 16. The system operator of the Private Sector BBS attempted to attend along with reporters from 2600. They were effectively thrown off the premises. Threats were made to charge them with trespassing and other crimes. An officer who had at first received them civilly was threatened with the loss of his job if he didn't get them removed promptly. Then the car was chased out of the parking lot. Perhaps prosecutor Alan Rockoff was afraid that he presence of some technically literate reporters would ruin the effect of his press release on the public. As it happens, he didn't need our help.

The next day the details of the press conference were reported to the public by the press. As Rockoff intended, paranoia about hackers ran rampant. Headlines got as ridiculous as hackers ordering tank parts by telephone from TRW and moving satellites with their home computers in order to make free phone calls. These and even more exotic stories were reported by otherwise respectable media sources. The news conference understandably made the front page of most of the major newspapers in the US, and was a major news item as far away as Australia and in the United Kingdom due to the sensationalism of the claims. We will try to explain why these claims may have been made in this issue.

On July 18 the operator of The Private Sector was formally charged with"computer conspiracy" under the above law, and released in the custody of his parents. The next day the American Civil Liberties Union took over his defense. The ACLU commented that it would be very hard for Rockoff to prove a conspiracy just "because the same information, construed by the prosecutor to be illegal, appears on two bulletin boards." especially as Rockoff admitted that "he did not believe any of the defendants knew each other." The ACLU believes that the system operator's rights were violated, as he was assumed to be involved in an illegal activity just because of other people under investigation who happened to have posted messages on his board.

In another statement which seems to confirm Rockoff's belief in guilt by association, he announced the next day that "630 people were being investigated to determine if any used their computer equipment fraudulently." We believe this is only the user list of the NJ Hack Shack, so the actual list of those to be investigated may turn out to be almost 5 times that. The sheer overwhelming difficulty of this task may kill this investigation, especially as they find that many hackers simply leave false information. Computer hobbyists all across the country have already been called by the Bound Brook, New Jersey office of the FBI. They reported that the FBI agents used scare tactics in order to force confessions or to provoke them into turning in others. We would like to remind those who get called that there is nothing inherently wrong or illegal in calling any ANY BBS, nor in talking about ANY activity. The FBI would not comment on the case as it is an "ongoing investigation" and in the hands of the local prosecutor. They will soon find that many on the Private Sector BBS's user list are data processing managers, telecommunications security people, and others who are interested in the subject of the BBS, hardly the underground community of computer criminals depicted at the news conference. The Private Sector BBS was a completely open BBS, and police and security people were even invited on in order to participate. The BBS was far from the "elite" type of underground telecom boards that Rockoff attempted to portray.

Within two days, Rockoff took back almost all of the statements he had made at the news conference, as AT&T and the DoD [Department of Defense - Shark] discounted the claims he had made. He was understandably unable to find real proof of Private Sector's alleged illegal activity, and was faced with having to return the computer equipment with nothing to show for his effort. Rockoff panicked, and on July 31, the system operator had a new charge against him, "wiring up his computer as a blue box." Apparently this was referring to his Novation Applecat modem which is capable of generating any hertz tone over the phone line. By this stretch of imagination an Applecat could produce a 2600 hertz tone as well as the MF which is necessary for "blue boxing." However, each and every other owner of an Applecat or any other modem that can generate its own tones therefore has also "wired up his computer as a blue box" by merely installing the modem. This charge is so ridiculous that Rockoff probably will never bother to press it. However, the wording of WIRING UP THE COMPUTER gives rockoff an excuse to continue to hold onto the computer longer in his futile search for illegal activity.

"We have requested that the prosecutors give us more specific information," said Arthur Miller, the lawyer for The Private Sector. "The charges are so vague that we can't really present a case at this point." Miller will appear in court on August 16 to obtain this information. He is also issuing a demand for the return of the equipment and, if the prosecutors don't cooperate, will commence court proceedings against them. "They haven't been particularly cooperative," he said.

Rockoff probably will soon reconsider taking Private Sector's case to court, as he will have to admit he just didn't know what he was doing when he seized the BBS. The arrest warrant listed only "computer conspiracy" against Private Sector, which is much more difficult to prosecute than the multitude of charges against some of the other defendants, which include credit card fraud, toll fraud, the unauthorized entry into computers, and numerous others.

Both Rockoff and the ACLU mentioned the Supreme Court in their press releases, but he will assuredly take one of his stronger cases to test the new New Jersey computer crime law. by seizing the BBS just because of supposed activities discussed on it, Rockoff raises constitutional questions. Darrell Paster, a lawyer who centers much of his work on computer crime, says the New Jersey case is "just another example of local law enforcement getting on the bandwagon of crime that has come into vogue to prosecute, and they have proceeded with very little technical understanding, and in the process they have abused many people's constitutional rights. What we have developing is a mini witch hunt which is analogous to some of the arrests at day care centers, where they sweep in and arrest everybody, ruin reputations, and then find that there is only one or two guilty parties." We feel that law enforcement, not understanding the information on the BBS, decided to strike first and ask questions later.

2600 magazine and the sysops of the Private Sector BBS stand fully behind the system operator. As soon as the equipment is returned, the BBS will go back up. We ask all our readers to do their utmost to support us in our efforts, and to educate as many of the public as possible that a hacker is not a computer criminal. We are all convinced of our sysop's innocence, and await Rockoff's dropping of the charges.

Note Readers will notice that our reporting of the events are quite different than those presented in the media and by the Middlesex County Prosecutor. We can only remind you that we are much closer to the events at hand than the media is, and that we are much more technologically literate than the Middlesex County Prosecutor's Office. The Middlesex County Prosecutor has already taken back many of his statements, after the contentions were disproven by AT&T and the DoD. One problem is that the media and the police tend to treat the seven cases as one case, thus the charges against and activities of some of the hackers has been extended to all of the charged. We at 2600 can only speak about the case of Private Sector.

Chapter 4

By now I assume that the reader has a fair idea of what phreaking is, and know a little bit about how to go about it. From now on, I will assume that the reader has read all the material before this or understands all the material covered. Now we will take a journey into the "Basics of Telecommunications" and learn a little about how everything works, and is related to everything else. This series of articles is extremely good and should be read by all levels of phreaks.

As we go further into the advanced world of phreaking, we come closer to the edge of technology. As we approach it, everything seems to become larger and more complicated. We notice that many things that were possible aren't anymore. Blue boxing is starting to become the only method of exploration as Equal Access looms nearer and nearer. As it stands now, equal access is here, and many LD services such as Sprint and MCI will be tougher to hack. Extenders will become more used and abused, which will cause them to get access codes miles long...

Blue boxing becomes harder as all Bell switching and transmission facilities go under to CCIS. Then to further complicate things, digital microwave, fiber optic, and satellite transmission are all coming to be digital and do not recognize 2600Hz for the hang up signal. I predict that around 1990, blue boxes will be obsolete from all major cities. A new type of box will have to be invented, or you'll have to get two fone line to phreak with, on to place the actual call and the other to tap into a COSMOS computer to change the status of the call from toll to toll-free, ie. 800#.

Well somethings will change for the better, with ISDN you'll get 144k bps lines and some other neat stuff.

Basic Telecommunications
Part II

BIOC Agent 003

Preface

In part II, we will explore the various special Bell#'s, such as: CN/A, AT&T newslines, loops, 99xx #'s, ANI, ringback, and a few others.

CN/A

CN/A, which stands for customer name and address, are bureaus that exist so that authorized Bell employees can find out the name and address of any customer in the Bell system. All #'s are maintained on file including unlisted #'s.

Here's how it works:

1) you have a # and you want to find out who owns it, e.g. (914) 555-1234.

2) You look up the CN/A # for that NPA in the list below. In the example, the NPA is 914 and the CN/A# is 518-471-8111.

3) You then call up the CN/A # (during business hours) and say something like, "hi, this is john jones from the residential service center in miami. Can I have the customer's name at 914-555-1234. That # is 914-555-1234." make up your own real sounding name, though.

4) If you sound natural & cheery, the operator will ask no questions.

Here's the list:

NPA	CN/A #	NPA	CN/A #
201	201-676-7070	517	313-232-8690
202	202-384-9620	518	518-471-8111
203	203-789-6800	519	416-487-3641
204	****n/a*****	601	601-961-0877
205	205-988-7000	602	303-232-2300
206	206-382-8000	603	617-787-2750
207	617-787-2750	604	604-432-2996
208	303-232-2300	605	402-345-0600
209	415-546-1341	606	502-583-2861
212	518-471-8111	607	518-471-8111
213	213-501-4144	608	414-424-5690
214	214-948-5731	609	201-676-7070
215	412-633-5600	612	402-345-0600
216	614-464-2345	613	416-487-3641
217	217-525-7000	614	614-464-2345
218	402-345-0600	615	615-373-5791
219	317-265-7027	616	313-223-8690
301	301-534-11??	617	617-787-2750
302	412-633-5600	618	217-525-7000
303	303-232-2300	701	402-345-0600
304	304-344-8041	702	415-546-1341
305	912-784-9111	703	804-747-1411
306	****N/a*****	704	912-784-9111
307	303-232-2300	705	416-487-3641
308	402-345-0600	707	415-546-1341
309	217-525-7000	709	****n/a*****
312	312-769-9600	712	402-345-0600
313	313-223-8690	713	713-658-1793
314	314-436-3321	714	213-995-0221
315	518-471-8111	715	414-424-5690
316	816-275-2782	716	518-471-8111
317	317-265-7027	717	412-633-5600
318	318-227-1551	801	303-232-2300
319	402-345-0600	802	617-787-2750

401	617-787-2750	803	912-784-9111
402	402-345-0600	804	804-747-1411
403	403-425-2652	805	415-546-1341
404	912-784-9111	806	512-828-2502
405	405-236-6121	807	416-487-3641
406	303-232-2300	808	212-226-5487
408	415-546-1341		bermuda only
412	412-633-5600	809	212-334-4336
413	617-787-2750	812	317-265-7027
414	414-424-5690	813	813-228-7871
415	415-546-1132	814	412-633-5600
416	416-487-3641	815	217-525-7000
417	314-436-3321	816	816-275-2782
418	514-861-6391	817	214-948-5731
419	614-464-2345	819	514-861-6391
501	405-236-6121	901	615-373-5791
502	502-583-2861	902	902-421-4110
503	503-241-3440	903	****n/a*****
504	504-245-5330	904	912-784-9111
505	303-232-2300	906	313-223-8690
506	506-657-3855	907	****n/a*****
507	402-345-0600	912	912-784-9111
509	206-382-8000	913	816-275-2782
512	512-828-2501	914	518-471-8111
513	614-464-2345	915	512-828-2501
514	514-861-6391	916	415-546-1341
515	402-345-0600	918	405-236-6121
516	518-471-8111	919	912-784-9111

Bell uses these #'s mainly to find out who owns a # that a customer claims he never called.

Note This is the most complete list of CN/A #'s in my possession (with only 5 #'s not available) this list was copyrighted in 1982 by "judas gerard" as it originally appeared in tap issue #78.

AT&T Newslines

Newslines are recordings that Bell employees call up to find out the latest info on stock, technology, etc. Concerning the Bell system.

Here are the #'s that are currently known to phreaks (at least me, anyway):

201-483-3800	nj	513-421-9060	oh
203-771-4920	ct	516-234-9914	ny
212-393-2151	ny	518-471-2272	ny
213-621-4141	ca	617-955-1111	ma
213-829-0111	ca (GTE)	702-789-6711	nv
213-449-8830	ca	713-224-6116	tx
312-368-8000	il	714-238-1111	ca
313-223-7223	mi	717-255-5555	pa
314-247-5511	mo	717-787-1031	pa
408-493-5000	ca	802-955-1111	ve
412-633-3333	pa	808-533-4426	hi
414-678-3511	wi	813-223-5666	fl
416-929-4323	ont.	914-948-8100	Ny
503-228-6271	or	916-480-8000	ca

Loops

First of all, you must understand the concept of loops. I think that the best way that this is understood is the way that phred phreek explained it...

> "no self-respecting phone phreak can go through life without knowing what a loop is, how to use one, and the types that are available. The loop is a great alternative communication medium that has many potential uses that haven't even been tapped yet. In order to explain what a loop is, it would be helpful to visualize two phone numbers (lines) just floating around in the telco central office (co).
>
> "Now, if you (and a friend perhaps) were to call these two numbers at the same time, poooopfff!, you are now connected together. I hear what you're saying out there..., "big deal" or "why should ma Bell collect here two msu's (message units) for one lousy phone call!?" well... Think again. Haven't you ever wanted someone to call you back but, were reluctant to give out your home phone number (like the last time you tried to get your friend's

> unlisted # from the business office)? Or how about a collect call to your friend waiting on a loop, who will gladly accept the charges? Or better yet, stumbling upon a loop that you discover that has multi-user capability (for those late-night conferences). Best of all is finding a non-supervised loop that doesn't charge any msu's or tolls to one or both parties.
>
> "Example: many moons ago, a loop affectionately known as 'the 332 loop' was non-sup (ie, non-supervised) on the tone side. I had my friend in california dial the free (non-sup) side, (212) 332-9906 and I dialed the side that charged, 332-9900. As you can see, I was charged one msu, and my friend as charged zilch, for as long as we wished to talk!"

Ahhh...have I perked your interest yet? If so, here is how to find a loop of you very own. First, do all of you loop searching at night! This is because the loops serve a genuine test function which telco uses during the day. (We don't want to run into an irate lineman now, do we?) to find a loop, having 2 #'s is a definite plus. If not, have a friend to dial #'s at his location. Last resort, try dialing from two adjacent pay phones. Now get your trusty white pages (*), and turn to the page where it lists the # of msu's from your exchange (or exchanges in your primary calling area) the idea is to find a loop that is within your primary calling area or is only 1 msu in your area (call area a). This is so you don't go bankrupt trying to find a loop. Write down all of these exchanges and do a 99xx scan of those exchanges (99xx scanning will be discussed shortly).

Before we get up to 99xx scanning, we will look at some other loop info:

Loops are found pairs which are usually close to each other. For example, in NPA 212, where the infamous loops are found, there is a standard loop format:

manhattan & bronx	NXX-9977/9979
brooklyn & queens	NXX-9900/9906

NXX is the exchange to be scanned. Here are some loops that have been found in nyc. These are used mostly by phreaks and call-in lines for pirate radio stations:

212-220-9900 / 9906
212-283-9977 / 9979
212-352-9900 / 9906
212-365-9977 / 9979
212-529-9900 / 9906
212-562-9977 / 9979
212-982-9977 / 9979
212-986-9977 / 9979

The lower # is the tone side (singing switch). The higher # is always silent. The tone disappears on the lower # when somebody dials in the other side of the loop. If you are on the higher #, you'll have to listen to the clicks to see if somebody dialed-in. The nyc 982 & 986 loops are different from others. Usually when you park on a loop, you will hear who ever calls in on the other half. When they're done, the next caller (if any) will be queued in, one after another. On the nyc 982 & 986, you sometimes can't get any more callers in after the first. Furthermore, if you park one of these loops and there is nobody on the other end for more than 4 minutes, you may be automatically disconnected. These loops are good for back-up purposes when all other loops are busy.

99xx Scanning

Most every exchange in the Bell system has a wide variety of test #'s and other "goodies," such as loops. These "goodies" are usually found between 9900 and 9999 in your local exchange. If you have the time and initiative, scan your exchange and you may become lucky!

Here are my findings in the 914-268:

9901	verification (recording of a/c and exchange)
9936	voice # to the telco co
9937	voice # to the telco co
9941	carrier
9960	osc. Tone (tone side loop)
9963	tone (stops: muted)
9966	carrier
9968	tone that disappears--responds to certain touch-tone keys

Most of the #'s between 9900 & 9999 will ring, be busy, go to a special intercept operator ("what #, please?"), or will go to a "the # you have reached..." recording. What you find depends upon the switching equipment in the exchange and the telco operating company.

When searching for loops, you may find one of the following possibilities when you find one:

1. You can hear through the loop (not muted), but there is a 1/2 second click every 10 seconds that interrupts the audio. This type is good for back-up use but the fucking click is super annoying.

2. One side of the loop is busy; try it again later.

3. The tone disappears, but you cannot hear through it (the loop is muted, try again in a month or so)

4. You get "the # you have reached recording." no loop here!

Most loops are muted (#3), but their status does changes from time-to-time. It all depends if the telco maintenance personnel remember to "throw the switch", ie, turn off the loop.

Since I have done the above 914-268 99xx scan, congers (268) has installed new switching equipment (dms100). Some of the numbers are the same, but I have noticed that on the dms100, the recordings are also stored in this area. 268-9903, 9906, 9909, & 9912 Are all different recordings. Also, there are 2 fortress fone recordings at 268-9911 (deposit 5 cents or else) and 268-9913 (deposit 10 cents). None of these recordings supe and alot of other 99xx#'s don't supe either.

In some areas (like md), 9906-7 is ringback. In washington, there is a sweep tone test at (202) 560-9944. In nyc (212), you'll find the infamous loop lines (as mentioned above).

It will be easier to scan your exchange if you make up a chart like the one below:

npa-NXX-99xx scan

99x x>	0	1	2	3	4	5	6	7	8	9
990										
991										
992										
993										
994										
995										
996										
997										
998										
999										

This leaves you with 100 boxes (1 for each # between 9900 & 9999). You should make your boxes big enough so you can write some sort of shorthand in them. For example:

```
  b  busy (try again at another time)
  r  rings (try again at another time)
  o  intercept operator ("what # you calling?)
 r1  recording 1 (make a margin note of the types of
     recordings you get)
  t  tone ] tone at a lower # + ignore
  i  ignore ] at a higher # = loop
  v  voice # to telco co - they usually answer with the
     city name or area.
  c  carrier
```

There will be others and you should use other characters that you can understand.

Now, back to loops! As you may have noticed in my 914-268 scan, I found a muted loop and a tone side. 914-268 Failed to come up with the silent side of a loop! Therefore, there is no loop in that exchange. I then scanned another exchange in my primary calling area (914-634) and I found a loop! "(914) 634-9923/9924" So, if at first you don't succeed, move onto another exchange. If you use the box method that I have outlined above, you will see a "t" & "i" next to each other for a loop.

Some exchanges are special. For example, 914-623 is a testing bureau. In this exchange, not only did I find a loop, but I also found several interesting tones, noises, and other test functions. Also, the more important the exchange is, the more you will find. For example, in 914-623, I found well over 10 voice #'s!

Also, loops are usually, but not exclusively, found in the 99xx series. For example: "(713) 324-1799/1499" is a loop.

The perfect loop? Here is what I would look for:

1. Non-sup on one or both sides. To check for a non-sup loop, go to a tone-first fortress fone and dial the #. If it asks for a dime, it is supervised. If the call goes through, then it is non-suped!

2. 800 Loops would be a plus. They are not necessarily found between 9900 & 9999 though. I would check the 1xxx series first.

3. Multi-user loops are also a plus for those late night conferences.

Finally, remember it is only a local call to find out what you co has in store for you. If you find anything interesting, be sure to drop me a line.

Note your local white pages can be a valuable asset. You can also order other fone books from your business office (usually free for books within your operating company's district). A large fone book, such as manhattan, contains much more info in the first few pages than other books.

ANI

Automatic number identification (ANI), is a number that you call up that will tell you what # you are calling from.

This has a few uses. First, were you ever somewhere and the fone didn't have a # printed on it? Or perhaps you were fooling around in some cans (those large boxes on fone poles that contain terminals for lineman use--to be discusses in a future chapter.) and you want to know what what the line # is. In NPA 914, the ANI is 990. In npa's 212 & 516, ANI is 958. This varies from area to area.

Here are some other ANI's that I have seen:

890-751-5191
202-222-2222
1-xxx-1111 (in some 914 areas, esp. Under step-by-step switching, you have to dial 1-990-1111)

To find ANI for other areas, check 3 digits #'s first, usually in the 9xx series (excluding 911). In areas under step-by-step (to be discussed in the next part), try 1-9xx-1111.

ANI may also be in 99xx. Last resort, try to get friendly with your neighbor who works for the fone company.

Ring Back

Ringback, as its name implies, calls back the # you are at when you dial the ringback #. Ringback, in NPA 914, is 660. You dial 660+the last 4 digits of the fone. You will then get a tone, hang-up quickly and pick-up in about 2 seconds. You will then get a second tone, hang-up again and the fone will ring.

In nyc, it is also 660, but you may have to press 6 or 7 before you hang up for the first time (ie, at the first tone).

Other ringback #'s that I have seen are:

26011 this 5 digit format is used primarily on step-by-step. The last 2 digits (11) are dummy digits.

890-897-xxxx xxxx are the last 4 digits of the fone #.

119911/11911/1199911	GTE
NXX-9906/9907	NPA 301, NXX is the exchange

The reason you get the tone when you pick-up after it rings is because in some areas, people were using ringback as an in-house intercom. They would dial ringback, and when it stopped ringing, they would pick-up & talk with the person who picked up the other extension. Bell didn't like this since there is usually only 1 piece of equipment in each exchange that does the ringback. When people used this as an intercom, linemen & repairmen couldn't get through! In some areas, especially those under step-by-step, ringback can still be used as an intercom. Also, under step-by-step, the ringback procedure it usually simple. For example, in one area you would dial 26011 and hang-up; it would then ringback.

Touch-Tone Test

In areas that have a touch-tone test, you dial the ringback #. At the first tone, you touch-tone digits 1-0. If they are correct it will beep twice. I have also seen a tt test in some areas at: 890-751-5191

Coming Soon

In the next part, we will look at various switching equipment and the network.

Break Up of Bell

The operating companies are not going to change all the switching equipment around. While there will be some changes, most of the information provided here will remain pertinent after january 1, 1984. Just substitute the word "fone network" for Bell system.

au revoir,

BIOC Agent 003
december 8, 1983

<<> G-File: The Official Phreakers Manual: PHREAK*.DOC 133
G_PHREAK.WPS 11/20/90 11:29 AM

Acknowledgements

Tap, Phred Phreek, Judas Gerard, The Magician, Dark Priest, & Myself.

I would also like to thank the Mulcher][for his assistance in distributing this tutorial.

Basic Telecommunications
Part III

BIOC Agent 003

Preface

In part III, we will discuss the dialing procedures for domestic as well as international dialing. We will also take a look at the telephone numbering plan.

North American Numbering Plan

In North America, the telephone numbering plan is as follows:

a) a 3 digit numbering plan area (NPA) code, [ie, area code]

b) a 7 digit telephone # consisting of a 3 digit central office (co) code plus a 4 digit station #.

These 10 digits are called the network address or destination code. It is in the format of:

```
    area code  telephone #

          n*x  nxx-xxxx
```

```
   where    n  a digit from 2-9
            *  the digit 0 or 1
            x  a digit 0-9
```

Area Codes

Check your telephone book or the separate listing of area codes found on many BBS's. Here are the special area codes (sac's):

510	twx (usa)
610	twx (canada)
700	new service
710	twx (usa)
800	wats
810	twx (usa)
900	dial-it services
910	twx (usa)

The other area codes never cross state lines, therefore each state must have at least one exclusive NPA code. When a community is split by a state line, the co #'s are often interchangeable (ie, you can dial the same # from 2 different area codes)

TWX

TWX (telex II) consists of 5 teletype-writer area codes. They are owned by western union. These sac's may only be reached via other TWX machines. These run at 110 baud. Besides the TWX #'s, these machines are routed to normal telephone #'s. Twx machines always respond with an answerback. For example, wu's fyi TWX # is (910) 988-5956, the corresponding real number to this is (201) 279-5956. The answerback for this service is "wu fyi mawa."

If you don't want to buy a TWX machine, you can still send TWX messages using easylink [800/325-4112 - see tuc's and my article entitled "hacking western union's easylink]

700

At the time of this writing, the 700 exchange does not yet exist. At&t plans to use it soon though. They plan to make it a type of fancy call forwarding service. It will be targeted towards salesmen on the run.

To understand how it works, i'll explain it with an example. Let's say joe q. Salespig works for AT&T security and he is on the run chasing a phreak around the country who royally screwed up an important COSMOS system. Let's say that joe's 700 # is (700) 382-5968. Every time joe goes to a new hotel, he dials a special 700 #, enters a code, and the # where he is staying. Now, if his boss received some important info, all he would do is dial (700) 382-5968 and it would ring wherever joe last programmed it to. Neat, huh?

800

This sac is one of my favorites since it allows for toll-free calls.

Inward wats (inwats): inward wide area telecommunications service is the 800 #'s that we are all familiar with. 800 #'S are set up in service areas or bands. There are 6 of these.

Band 6 is the largest and you can call a band 6 # from anywhere in the us except the state where the call is terminated (this is why most companies have one 800 # for the country and then another for just one state). Band 5 includes the 48 contiguous states. All the way down to band 1 which includes only the states contiguous to that one. Therefore, less people can reach a band 1 inwats # that a band 6 #.

Intrastate inwats #'s (ie, you can call it from only 1 state) always have a 2 as the last digit in the exchange (ie, 800-nx2-xxxx). The nxx on 800 #'s represent the area where the business is located. For example, a # beginning with 800-431 would terminate at a new york co.

800 #'s always end up in a hunt series in a co. This means that it tries the first # allocated to the company for their 8p0 lines; if this is busy it will then try the next #, etc). You must have a minimum of two lines per each 800 #. For example, travelnet uses a hunt series. If you dial (800) 521-8400, it will first try the # associated with 8400; if it is busy it will go to the next available port, etc. Inwats customers are billed by the # of hours of calls that are made to their #.

Outwats (outward wats): outwats are for making outgoing calls only. Large companies use outwats since they receive bulk-rate discounts. Since outwats # cannot have incoming calls, they are in the format of:

(800) *xx-xxxx

Where * is the digit 0 or 1 which cannot be dialed unless you box the call. The *xx identifies the type of service and the areas that the company can call.

Remember: inwats + outwats = wats extender (see part I)

900

This dial-it sac is a nationwide dial-it service. It is used for taking television polls and other stuff. The first minute currently costs an outrageous 50 cents and each additional minute costs 35 cents. Bell takes in alot of revenue in this way.

Dial (900) 555-1212 to find out what is currently on the service.

CO Codes

These identify the switching office where the call is to be routed. The following co codes are reserved nationwide:

555	directory assistance	
844	time \	these are now in
936	weather /	the 976 exchange
950	future services	
958	plant test	
959	plant test	
970	plant test (temporary)	
976	dial-it services	

Also, the 3 digit ANI & ringback #'s are regarded as plant test and are thus reserved. These numbers vary from area to area.

950
(also see part I)

Here are the services that are currently on the 950 exchange:

1000	spc
1022	MCI execunet
1033	us telephone
1044	allnet
1066	lexitel
1088	sbs skyline

These scc's (specialized common carriers) are free from fortresses!

Publishers note: Most 950's now require the station code (1022, 1000, 1088, etc.) to be five digits long. Mci 950-10222, us telefone 10333, allnet 10444, etc. Look in "equal access and the american dream" p. for a complete list.

Plant Tests

These include ANI, ringback, and other various tests.

976

Dial 976-1000 to see what is currently on the service. Also, many BBS's have a listing of these #'s.

N11 Codes

Bell is trying to phase some of these out, but they still exist in many areas.

011	international dialing prefix
211	coin refund operator
411	directory assistance
611	repair service
811	business office
911	emergency

International Dialing

With international dialing, the world has been divided into 9 numbering zones. To make an international call, you must dial: int. Prefix + country code + nat. #

In north america, the international dialing prefix is 011 for station-to-station calls and 01 for operator- serviced calls. Iddd stands for international direct distance dialing.

The country code, which varies from 1 to 3 digits, always has the world numbering zone as the first digit. For example, the country code for the united kingdom is 44, thus it is in world numbering zone 4.

Some boards may contain a complete listing of other country codes, but here are a few:

001	north america (us, canada,etc)
020	egypt
258	mozambique
034	spain
049	germany
052	mexico (southern portion)
061	australia
007	ussr
081	japan
098	iran

If you call from an area other than north america, the format is generally the same. For example, let's say you wanted to call the white house from switzerland. First you would dial 00 (the swiss international dialing prefix), then 1 (the us country code), followed by 202-456-1414 (the national # for the white house).

Also, country code 87 is reserved for maritime mobile service, ie calling ships:

871	marisat (atlantic)
872	marisat (pacific)
873	marisat (indian)

International Switching

In north america, there are currently 7 no. 4 Ess's that perform the duty of isc (international switching centers). All international calls dialed from numbering zone 1 will be routed through one of these "gateway cities." they are:

182	White Plains, ny
183	New York, ny
184	Pittsburgh, pa
185	Orlando, fl
186	Oakland, ca
187	Denver, co
188	New York, ny

The 18x series are operator routing codes for overseas access (to be further discussed with blue boxes). All international calls use a signaling system called ccitt. It is an international standard for signaling.

Coming Soon

In part IV, we will discuss switching equipment, various operators, co types, etc.

Phreaking lives in '84,

BIOC Agent 003

fargo 4a
23-feb-84

References,
Acknowledgements

- Notes on the network (AT&T)
- Tap (room 603, 147w 42 ST, new york, ny 10036)
- Understanding Telephone Electronics
- and many others / Tuc, Mulcher...

Basic Telecommunications
Part IV

BIOC Agent 003

Preface

Part IV will deal with the various types of operators, office hierarchy, & switching equipment.

Operators

There are many types of operators in the network and the more common ones will be discussed.

TSPS Operator

The TSPS (traffic service position system) operator is probably the bitch (or bastard for the phemale liberationists) that most of us are use to having to deal with.

Here are her responsibilities:

1) obtaining billing information for calling card or 3rd number calls.

2) identifying called customer on person-to-person calls.

3) obtaining acceptance of charges on collect calls.

4) identifying calling numbers. This only happens when the calling # is not automatically recorded by cama (centralized automatic message accounting) & forwarded from the local office. This could be caused by equipment failures or if the office is not equipped for cama (most are).

> <u>I once had an equipment failure happen to me & the TSPS operator came on and said, "what # are you calling from?" out of curiosity, I gave her the # to my co, she thanked me & then I was connected to a conversion that appeared to be between a fire man & his wife. Then it started ringing the party I originally wanted to call & everyone phreaked out (excuse the pun). I immediately dropped this dual line conference!</u>

You shouldn't mess with the TSPS operator since she knows where you are calling from. She also knows whether or not you are at a fortress fone & she can trace calls quite readily. Out of all the operators, she is one of the most dangerous.

Inward Operator

This operator assists your local TSPS ("0") operator in connecting calls. She will never question a call as long as the call is within her service area. She can only be reached via other operators or by a blue box. From a bb, you would dial KP+NPA+121+ST for the inward operator that will help you connect any calls within that NPA area only. (Blue boxing will be discussed in a future part of basic telcom)

Directory Assistance Operator

This is the operator that you are connected to when you dial: 411 or npa-555-1212. She does not readily know where you are calling from. She does not have access to unlisted #'s, but she does know if an unlisted # exists for a certain listing.

There is also a directory assistance for deaf people who use teletypewriters if you modem can transfer baudot (the apple cat can), then you can call her up and have an interesting conversation with her. The # is:800/855-1155. She uses the standard telex abbreviations such as ga for go ahead. They tend to be nicer & will talk longer than your regular operators. Also, they are more vulnerable into being talked out of information through the process of "social engineering" as cheshire catalyst would put it.

Other operators have access to their own da by dialing KP+NPA+131+ST (mf).

This is a little out of the scope of this tutorial, but many telco's are now charging for calls to dir. Asst. You can beat this by:

1. Count how many calls you make to directory assistance in a billing period. Go to a fortress fone & dial da. When the operator comes on, give her a name that you know has an unlisted # or ask for a town that isn't in the NPA. She will then ask for your # so she can credit the call to you. Give her your home #, she doesn't know that you are making a free call from the fortress. Just make sure that you don't credit yourself for more calls than you actually made or you might have a few problems!

2. If you have a baudot terminal, use the 800 #, it's free & there is one # for all requests.

C/NA Operators

C/NA operators are operators that do exactly the opposite of what directory assistance operators are for. See part II, for more info on C/NA & #'s. In my experiences, these operators know more than the da op's do & they are more susceptible to "social engineering." it is possible to bullshit a C/NA operator for the non-pub da # (ie, you give them the name & they give you the unlisted #). This is due to the fact that they assume your are a phellow company employee.

Intercept Operator

The intercept operator is the one that you are connected to when there are not enough recordings available to tell you that the # has been disconnected or changed. She usually says, "what # you callin' ? " With a foreign accent. This is the lowest operator lifeform. Even though they don't know where you are calling from, it is a waste of your time to try to verbally abuse them since they usually understand very little english.

Other Operators

And then there are the:

- o mobile

- o ship-to-shore
- o conference
- o marine verify, "leave word & call back,"
- o rout & rate (KP+NPA+141+ST) & other special operators who have one purpose or
- o another in the network.

Problems with an operator? Ask to speak to their supervisor... Which is the equivalent of the madame in a whorehouse (if you will excuse the analogy).

By the way, some co's that will allow you to dial a 1 or 0 as the 4th digit, will also allow you to call special operators without a blue box. This is very rare though! For example, 212-121-1111 will get you a ny inward operator.

Office Hierarchy

Every switching office office in north america (the NPA system), is assigned an office name & class. There are five classes of offices numbered 1 through 5. Your co is most likely a class 5 or end office. All long-distance (toll) calls are switched by a toll office which can be a class 4, 3, 2, or 1 office. There is also a 4x office called an intermediate point. The 4x office is a digital one that can have an unattended exchange attached to it (known as a remote switching unit-rsu).

The following chart will list the office #, name, & how many of those offices existed in north america in 1981:

class	name	abb	# existing
1	regional center	rc	12
2	sectional center	sc	67
3	primary center	pc	230
4	toll center	tc	1,30
4p	toll point	tp	?
4x	intermediate pt	ip	?
5	end office	eo	19,000
r	rsu	rsu	?

When connecting a call from one party to another, the switching equipment usually tries to find the shortest route between the class 5 end office of the caller & the class 5 end office of the called party. If no inter-office trunks exist between the 2 parties, it will then move upto the next highest office for servicing (class 4). If the class 4 office cannot handle the call by sending it to another class 4 or 5 office, it will be sent to the next office in the hierarchy (3). The switching equipment first uses the high-usage interoffice trunk groups, if they are busy it then goes to the final trunk groups on the next highest level. If the call cannot be connected then, you will probably get a re-order (120ipm busy signal) signal. At this time, the guys at network operations are probably shitting in their pants and trying to avoid the dreaded network dreadlock (as seen on tv!).

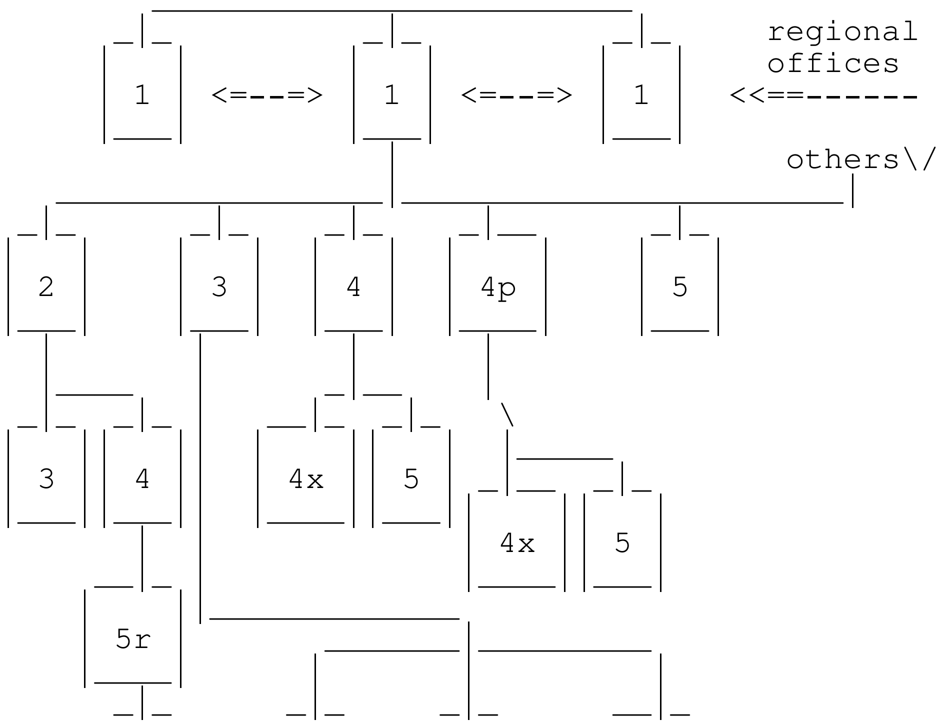
It is also interesting to note that 9 connections in tandem is called ring-around-the rosy and it has never occurred in telephone history. This would case an endless loop connection. [A neat way to really screw-up the network].

The 10 regional centers in the us & the 2 in canada are all interconnected. They form the foundation of the entire telephone network. Since there are only 12 of them, they are listed below:

class 1 regional office location	NPA
Dallas 4 ESS	214
Wayne, pa	215
Denver 4t	303
Regina no.2 sp1-4w (Canada)	306

St. Louis 4t	314
Rockdale, ga	404
Pittsburgh 4e	412
Montreal no.1 4aets (Canada)	504
Norwich, ny	607
San Bernardino, ca	714
Norway, il	815
White Plains 4t, ny	914

The following diagram demonstrates how the various offices may be connected:



```
|   |   |   |   |   |   |    |
| r |   | 4 |   | 5 |   | 5r |
|___|   |___|   |___|   |____|
```

Note The preceding diagram used special symbols from an apple //e that may not be viewed as I intended them if you are not using an apple//e or //c.

Switching Equipment

In the network, there are 3 major types of switching equipment. They are known as: step, crossbar, & ESS.

Step-by-Step (SxS)

The step-by-step, a/k/a the strowger switch or two-motion switch, was invented in 1889 by an undertaker named almon strowger. He invented this mechanical switching equipment because he felt that the biased operator was routing all requests for an 'undertaker' to her husband's business. Bell started using this system in 1918 as of 1978, over 53% of the Bell exchanges used this method of switching.

Step-by-step switching is controlled directly by the dial pulses which move a series of switches (called the switch train) in order. When you first pick up the fone under SxS, a linefinder acknowledges the request (sooner or later) by sending a dial tone. If you then dialed 1234, the equipment would first find an idle selector switch. It would then move vertically 1 pulse, it would then move horizontally to find a free second selector, it would then move 2 vertical pulses, step horizontally to find the next selector, etc. Thus the first switch in the train takes no digits, the second switch takes 1 digit, the third switch takes 1 digit, & the last switch in the train (called the connector) takes the last 2 digits & connects your calls. A normal (10,000 line) exchange requires 4 digits (0000-9999) to connect a local call & thus it takes 4 switches to connect every call (linefinder, 1st & 2nd selectors, & the connector) .

While it was the first, SxS sucks for the following reasons:

1. the switched often become jammed thus the calls often become blocked.

2. you can't use DTMF (dual-tone multi-frequency a/k/a touch-tone) directly. It is possible that the telco may have installed a conversion kit but then the calls will go through just as slow as pulse, anyway!

3. they use a lot of electricity & mechanical maintenance. (Bad from telco point of view)

4. everything is hardwired.

They can still hook up pen registers & other shit on the line so it is not exactly a phreak haven.

You can identify SxS offices by:

1. lack of DTMF or pulsing digits after dialing DTMF.

2. if you go near the co, it will sound like a typewriter testing factory.

3. lack of speed calling, call forwarding, & other customer services.

4. fortress fones that want your money first (as opposed to dial tone first ones).

The preceding don't necessarily imply that you have SxS but they surely give evidence that it might be. Also, if any of the above characteristics exist, it certainly isn't ESS! Also, SxS have pretty much been eradicated from large metropolitan areas such as nyc (212).

Crossbar

There are 3 major types of crossbar systems called: no. 1 Crossbar (1xb), no. 4 Crossbar (4xb), & no. 5 Crossbar (5xb). 5Xb has been the primary end office switch of Bell since the 60's and thus it is in wide-use.

Crossbar uses a common control switching method. When there is an incoming call, a stored program determines its route through the switching matrix.

In crossbar, the basic operation principle is that a horizontal & a vertical line are energized in a matrix known as the crosspoint matrix. The point where these 2 lines meet in the matrix is the connection.

ESS

Electronic switching system (ESS) the phreak's nightmare come true (or orwell's prophecy as 2600 puts it)

ESS is bell's move towards the airstrip one society depicted in orwell's 1984. With ESS, every single digit that you dial is recorded--even if it is a mistake. They know who you call, when you call, how long you talked for, & probably what you talked about (in some cases). Ess can (and is) also programmed to print out #'s of people who make excessive calls to 800 #'s or directory assistance. This is called the "800 exceptional calling report." ESS could also be programmed to print out logs of who calls certain #'s--like a bookie, a known communist, a BBS, etc the thing to remember with ESS is that it is a series of programs working together. These programs can be very easily changed to do whatever they want it to do. One phreak whom I know has some ESS source code listing which is incredibly complex (as well as documented--gracias dios). This system makes the job of Bell security, the FBI, NSA, & other organizations that like to invade privacy incredibly easy.

With ESS, tracing is done in microseconds (eine augenblick) & the results are printed at the console of a Bell gestapo officer. Ess will also pick up any "foreign" tones on the line such as 2600 Hz!

Bell predicts that the country will become totally ESS by the 1990's.

You can identify ESS by the following which are usually ESS functions:

1. dialing 911 for help.

2. dial-tone-first fortresses.

3. custom calling services such as:call forwarding, speed dialing, & call waiting. (Ask your business office if you can get these.)

4. ANI (automatic number identification) on LD calls.

Phreaking does not come to a complete halt under ESS though - just be very careful, though!

Due to the fact that ESS sends a computer generated "artificial ring," where the voice is not connected directly to the called parties line until he picks up, black boxes & infinity transmitters will not work!

Note another interesting way to find out what type of equipment you are on is to raid the trash can of you local co - this art will discussed in a separate article soon.

Coming Soon

In the part V, we will start to take a look at telephone electronics.

Further Reading

For more information on the above topics, I suggest the following:

- o notes on the network, AT&T, 1980.
- o understanding telephone electronics,texas instruments, 1983.

and subscriptions to:

- o tap, room 603, 147 w 42 ST, new york, ny 10036. Subscriptions are $10/year.#back issues are $0.75. The current issues is #90 (jan/feb 1984)
- o 2600, box 752, middle island, ny 11953. Subscriptions are $10/year. Backissues are $1 each. The current issue is #4 (april 1984).

They are both excellent sources of all sorts of information (primarily phreaking/hacking).

Note for the most part, I have assumed that you have read my previous 3 courses in the basic telcom series.

hasta luego,

BIOC Agent 003
april 13, 1984 [the year of big brother]

Fargo 4A

Basic Telecommunications
Part V

BIOC Agent 003

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. Here-in-after 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 sires 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-9.

In telephony, the red & green wires are often referred to as tip (t) & ring (r). The tip is usually 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 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 rectifier bridge which compensates for polarity reversal.] this I 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 generated.

Voltages, etc.

When your telephone is on-hook (ie, hung up) there is approximately 48 volts of DC current (vDC) flowing through 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 13 volts. The resistance of the loop also drops below the 2500 ohm level.

As of now, you are probably saying to yourself that this is all nice and technical but what the hell good is the information. Well, also consider that this voltage (& resistance) drop is how the co detects that a fone was taken off hook (picked up). In this way, they know when to start billing the calling number. Now what do you suppose would happen if a device such as a resistor or a zener diode was placed on the called parties line so that the voltage would drop just enough to allow talking but not enough to start billing? First off, the calling party would not be billed for the call but conversation could be pursued. Secondly, the co equipment would think that the fone just kept on ringing. The telco calls this a "no-no" (toll fraud to be more specific) while phone phreaks affectionately 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 one or 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 the 2 screws on the network box labeled >f< and >rr<. Wrap the resistor between the 2 screws making sure that it doesn't touch any other terminals!. Now connect one wire from the switch to the rr terminal. Finally, attach the remaining wire to the green 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 one second then put the switch in the free position and pick up the fone. Keep all call short and preferably under 15 minutes.

Note if anyone 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 signaling a phriend that you are about to call is making a collect call to a non-existent 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!

Pictorial diagram
(standard rotary k500 fone)

```
 _____________________________________
|                                      |
***blue wire**>>f<                     |
|            *   *                     |
**white wire**   *                     |
|                *                     |
|            resistor                  |
|                *                     |
|                *                     |
|              >rr<*******switch****   |
|                                  *   |
****green wire**********************   |
|                                      |
|_____________________________________|
```

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 (rms) of ac current down the line (at around 15 to 60 Hz) in standard 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. A regular 60 watt light bulb can also be hooked up using a simple (120 vac) relay.

Warning   90 & 120 vac can give quite a shock. Exercise extreme caution if you wish to further pursue these topics.

Also included in the ringing circuit is a capacitor to prevent the DC current from interfering with the Bell [a capacitor will pass ac current while it will prevent DC current from flowing (by storing it)].

Another reason that the telco hates black boxes is because ringing uses alot of common-control equipment, in the co, which use alot of electricity. Thus the ringing generators are being tied up while a free call is being made. Usually calls that are allowed to ring for a long period of time may be construed as suspicious. Some offices may be set up to drop a trouble card for long periods of ringing then a "no-no" detection device may be placed on the line.

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 (making) the local loop once for every 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, there are 10 pulses per second (max). 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) break period and a 40 ms make period. (60+40=100 Ms = 1/10 minute). This is referred to as a 60% break interval. Some of the more sophisticated electronic fones can switch between a 60% & a 67% break 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 switchook. (If you depress it for longer than a second it will be construed as a disconnect.) by rapidly switchooking you are causing the local loop to be broken & made similar to rotary dialing! Thus if you can manage to switchook rapidly 10 times you can reach an operator to place any call you want! This takes alot of practice, though. You might want to 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 noises 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 upto 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 697 Hz-	q 1	abc 2	def 3	a
770 Hz-	ghi 1	jkl 2	mno 3	b
852 Hz-	prs 1	tuv 2	wxy 3	c
941 Hz-	*	operator z 0	#	d

```
          |___________|___________|___________|___________|
                |           |           |           |
             1209 Hz     1336 Hz     1477 Hz     1633 Hz
               high group
```

A portable DTMF keypad is known as a white box.

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 key are called: flash, immediate, priority, & routine (with variations) instead of abcd. Secondly, these keys are used for testing purposes by the telco. In some area 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 ad 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 become 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) ad 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 current flowing 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.

The reason 2 sires are used on the local loops are because it is alot cheaper for the telco. Although, all of the inter-office trunks utilize 4 wires. This is necessary for full duplex (ie, simultaneous conversation on both sides) and for amplification devices. There are similar devices in the co's, known as a hybrid, that couple the 4-wire trunks to the 2-wire local loops and visa-versa.

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 switchook. 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:

```
     (red) o_________________________
      [l1]     |             |      |
               |             |      |
            1000 ohm         |      \
               |             |       \
            resistor       ringing  |
               |           circuit  |  -switch
               |             |      |     hook
               /             |      |
              / spst switch  |      \
               |             |       \
               |             |      |
               |             |      |
     (green) o__|_____________|______|
       [l2]
     --> to rest of fone
```

Conclusion

Note many of the electronics components of normal fones (k500)
     are enclosed in the network box (which shouldn't be
     opened).

I have assumed that the reader has a basic knowledge of electronics. Also, I have assumed that you have read the 4 previous installments of this series (and hopefully enjoyed them).

In part VI, we will take a look at fortress fones.

Suggested Further Reading

- electronics courses a-d, tap, @ $.75 each.
- electronic telephone projects, a.j. Caristi, howard sams books.
- everything you always wanted to know about 1633 Hz tones but were afraid to ask, the magician, tap, issue #62.
- free Bell phone calls, tap, fact sheet #2, @ $.50.
- free GTE phone calls, tap, fact sheet #3, @ $.50.
- how to modify your Bell touch tone fone to have 1633 cycle tones, tap, issue #63.
- modifying your phone for 1633 Hz (new electronic keypads), fred steinbeck, tap, issue #84.
- notes on the network, AT&T.
- the phone book, j. Edgar Hyde.
- regulating the telephone company in your home, ramapart magazine, june 1972.
- remobs, tap #91 (not yet published as of this writing).
- understanding telephone electronics, texas instruments.

& other assorted sources...

- tap, room 603/147 w 42 ST./new york, ny 10036. Please specify by backissue #'s (not article names). All back-issues are $1 each. Subscriptions are $10/year (10 issues). Say that bioc agent 003 sent you.

Basic Telecommunications
Part VI

BIOC Agent 003

Revised 27-OCT-84

Preface

This article will focus primarily on the standard Western Electric single-slot coin telephone (aka fortress fone) which can be divided into 3 types:

- o Dial-Tone First (DTF)
- o Coin-First (CF): (ie, it wants your $ before you receive a dial tone)
- o Dial Post-Pay Service (PP): you pay after the party answers

Depositing Coins (Slugs)

Once you have deposited your slug into a fortress, it is subjected to a gamut of tests. The first obstacle for a slug is the magnetic trap. This will stop any light-weight magnetic slugs and coins. If it passes this, the slug is then classified as a nickel, dime, or quarter. Each slug is then checked for appropriate size and weight. If these tests are passed, it will then travel through a nickel, dime, or quarter magnet as appropriate. These magnets set up an eddy current effect which causes coins of the appropriate characteristics to slow down so they will follow the correct trajectory. If all goes well, the coin will follow the correct path (such as bouncing off of the nickel anvil) where it will hopefully fall into the narrow accepted coin channel.

The rather elaborate tests that are performed as the coin travels down the coin chute will stop most slugs and other undesirable coins, such as pennies, which must then be retrieved using the coin release lever.

If the slug miraculously survives the gamut, it will then strike the appropriate totalizer arm causing a ratchet wheel to rotate once for every 5-cent increment (eg, a quarter will cause it to rotate 5 times).

The totalizer then causes the coin signal oscillator to readout a dual-frequency signal indicating the value deposited to ACTS (a computer) or the TSPS operator. These are the same tones used by phreaks in the infamous red boxes.

For a quarter, 5 beep tones are outpulsed at 12-17 pulses per second (PPS). A dime causes 2 beep tones at 5 - 8.5 PPS while a nickel causes one beep tone at 5 - 8.5 PPS. A beep consists of 2 tones: 2200 + 1700 Hz.

A relay in the fortress called the "B relay" (yes, there is also an 'A relay') places a capacitor across the speech circuit during totalizer read-out to prevent the "customer" from hearing the red box tones.

In older 3 slot phones: one Bell (1050-1100 Hz) for a nickel, two bells for a dime, and one gong (800 Hz) for a quarter are used instead of the modern dual-frequency tones.

TSPS & ACTS

While fortresses are connected to the CO of the area, all transactions are handled via the Traffic Service Position System (TSPS). In areas that do not have ACTS, all calls that require operator assistance, such as calling card and collect, are automatically routed to a TSPS operator position.

In an effort to automate fortress service, a computer system known as Automated Coin Toll Service (ACTS) has been implemented in many areas. ACTS listens to the red box signals from the fones and takes appropriate action. It is ACTS which says, "Two dollars please (pause) Please deposit two dollars for the next ten seconds" (and other variations). Also, if you talk for more than three minutes and then hang-up, ACTS will call back and demand your money. ACTS is also responsible for Automated Calling Card Service.

ACTS also provide trouble diagnosis for craftspeople (repairmen specializing in fortresses). For example, there is a coin test which is great for tuning up red boxes. In many areas this test can be activated by dialing 09591230 at a fortress (thanks to Karl Marx for this information). Once activated it will request that you deposit various coins. It will then identify the coin and outpulse the appropriate red box signal. The coins are usually returned when you hang up.

To make sure that there is actually money in the fone, the CO initiates a "ground test" at various times to determine if a coin is actually in the fone. This is why you must deposit at least a nickel in order to use a red box!

Green Boxes

Paying the initial rate in order to use a red box (on certain fortresses) left a sour taste in many red boxer's mouths thus the GREEN BOX was invented. The green box generates useful tones such as COIN COLLECT, COIN RETURN, and RINGBACK. These are the tones that ACTS or the TSPS operator would send to the CO when appropriate. Unfortunately, the green box cannot be used at a fortress station but it must be used by the CALLED party.

Here are the tones

Coin Collect	700 + 1100 Hz
Coin Return	1100 + 1700 Hz
Ringback	700 + 1700 Hz

Before the called party sends any of these tones, an operator released signal should be sent to alert the MF detectors at the CO. This can be accomplished by sending 900 + 1500 Hz or a single 2600 Hz wink (90 ms) followed by a 60 ms gap and then the appropriate signal for at least 900 ms.

Also, do not forget that the initial rate is collected shortly before the 3 minute period is up.

Incidentally, once the above MF tones for collecting and returning coins reach the CO, they are converted into an appropriate DC pulse (-130 volts for return & +130 volts for collect). This pulse is then sent down the tip to the fortress. This causes the coin relay to either return or collect the coins.

The alleged "T-Network" takes advantage of this information. When a pulse for COIN COLLECT (+130 VDC) is sent down the line, it must be grounded somewhere. This is usually either the yellow or black wire. Thus, if the wires are exposed, these wires can be cut to prevent the pulse from being grounded. When the three minute initial period is almost up, make sure that the black & yellow wires are severed; then hang up, wait about 15 seconds in case of a second pulse, reconnect the wires, pick up the fone, hang up again, and if all goes well it should be "JACKPOT" time.

<<> G-File: The Official Phreakers Manual: PHREAK*.DOC   163
     G_PHREAK.WPS 11/20/90 11:29 AM

Physical Attack

A typical fortress weighs roughly 50 lbs. with an empty coin box. Most of this is accounted for in the armor plating. Why all the security? Well, Bell contributes it to the following:

> "Social changes during the 1960's made the multislot coin station a prime target for: vandalism, strong arm robbery, fraud, and theft of service. This brought about the introduction of the more rugged single slot coin station and a new environment for coin service."

As for picking the lock, I will quote Mr. Phelps:

> "We often fantasize about 'picking the lock' or 'getting a master key.' Well, you can forget about it. I don't like to discourage people, but it will save you from wasting alot of your time--time which can be put to better use (heh, heh)."

As for physical attack, the coin plate is secured on all four side by hardened steel bolts which pass through two slots each. These bolts are in turn interlocked by the main lock.

One phreak I know did manage to take one of the 'mothers' home (which was attached to a piece of plywood at a construction site; otherwise, the permanent ones are a bitch to detach from the wall!). It took him almost ten hours to open the coin box using a power drill, sledge hammers, and crow bars (which was empty -- perhaps next time, he will deposit a coin first to hear if it slushes down nicely or hits the empty bottom with a clunk.)

Taking the fone offers a higher margin of success. Although this may be difficult often requiring brute force and there has been several cases of back axles being lost trying to take down a fone! A quick and dirty way to open the coin box is by using a shotgun. In Detroit, after ecologists cleaned out a municipal pond, they found 168 coin phones rifled.

In colder areas, such as Canada, some shrewd people tape up the fones using duct tape, pour in water, and come back the next day when the water will have froze thus expanding and cracking the fone open.In one case:

> "unauthorized coin collectors" where caught when they brought $6,000 in change to a bank and the bank became suspicious...

At any rate, the main lock is an eight level tumbler located on the right side of the coin box. This lock has 390,625 possible positions (5 ^ 8, since there are 8 tumblers each with 5 possible positions) thus it is highly pick resistant! The lock is held in place by 4 screws. If there is sufficient clearance to the right of the fone, it is conceivable to punch out the screws using the drilling pattern below (provided by Alexander Mundy in TAP)

Chapter 5

What is covered in these last few articles, is the essence of phreaking, blue boxing & equal access. These last articles, I hope will be the final stage of phreak education for now. Basic telecommunications 7 is a brief intro to the art of blue boxing, while Better Homes & Blue Boxing will cover it in full. Equal access will be an interesting switch, it is installed in my area already and I have been investigating it. One thought is to call MCI operators and box through them, over MCI lines...

Basic Telecommunications
Part VII

BIOC Agent 003

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.

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 Signalling Principles

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, #he 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
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

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 is 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 does require a diode matrix keypad though, 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.

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."

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)."

<<> G-File: The Official Phreakers Manual: PHREAK*.DOC 173
G_PHREAK.WPS 11/20/90 11:29 AM

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 yourself (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, STP, ST3P, & 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 automatically just like the language assistance digit [which distinguishes operator (or blue box) dialed 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 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).

Coming soon

Telcom VIII will deal with cordless phones, mobile phones, and other neat things.

Be careful and have phun,

BIOC Agent 003

Better Homes and Blue Boxing
Part I: Theory of Operation

To quote Karl Marx, blue boxing has always been the most noble form of phreaking. As opposed to such things as using an MCI code to make a free fone call, which is merely mindless pseudo-phreaking, blue boxing is actual interaction with the Bell System toll network. It is likewise advisable to be more cautious when blue boxing, but the careful phreak will not be caught, regardless of what type of switching system he is under.

In this part, I will explain how and why blue boxing works, as well as where. In later parts, I will give more practical information for blue boxing and routing information.

To begin with, blue boxing is simply communicating with trunks. Trunks must not be confused with subscriber lines (or "customer loops") which are standard telefone lines. Trunks are those lines that connect central offices. Now, when trunks are not in use (i.e., idle or "on-hook" state) they have 2600Hz applied to them. If they are two-way trunks, there is 2600Hz in both directions. When a trunk IS in use (busy or "off-hook" state"), the 2600Hz is removed from the side that is off-hook. The 2600Hz is therefore known as a supervisory signal, because it indicates the status of a trunk; on hook (tone) or off-hook (no tone). Note also that 2600Hz denoted SF (single frequency) signalling and is "in-band." This is very important. "In-band" means that is is within the band of frequencies that may be transmitted over normal telefone lines. Other SF signals, such as 3700Hz are used also. However, they cannot be carried over the telefone network normally (they are "out-of-band") and are therefore not able to be taken advantage of as 2600Hz is.

Back to trunks. Let's take a hypothetical phone call. You pick up your fone and dial 1+806-258-1234 (your good friend in

Armarillo, Texas). For ease, we'll assume that you are on #5 Crossbar switching and not in the 806 area. Your central office (CO) would recognize that 806 is a foreign NPA, so it would route the call to the toll centre that serves you. [For the sake of accuracy here, and for the more experienced readers, note that the CO in question is a class 5 with LAMA that uses out-of-band SF supervisory signalling]. Depending on where you are in the country, the call would leave your toll centre (on more trunks) to another toll centre, or office of higher "rank". Then it would be routed to central office 806-258 eventually and the call would be completed.

Illustration:

```
     A -------- CO1 ----- TC1 ----- TC2 ----- CO2 ----- B


       A  you
     CO1  your central office
     TC1  your toll office
     TC2  toll office in Amarillo
     CO2  806-258 central office
       B  your friend (806-258-1234)
```

In this situation it would be realistic to say that CO2 uses SF in-band (2600Hz) signalling, while all the others use out-of-band signalling (3700Hz). If you don't understand this, don't worry too much. I am pointing this out merely for the sake of accuracy. The point is that while you are connected to 806-258-1234, all those trunks from YOUR central office (CO1) to the 806-258 central office (CO2) do *NOT* have 2600Hz on them, indicating to the Bell equipment that a call is in progress and the trunks are in use.

Now let's say you're tired of talking to your friend in Amarillo (806-258-1234) so you send a 2600Hz down the line. This tone travels down the line to your friend's central office (CO2) where it is detected. However, that CO thinks that the 2600Hz is originating from Bell equipment, indicating to it that you've hung up, and thus the trunks are once again idle (with 2600Hz present on them). But actually, you have not hung up, you have fooled the equipment at your friend's CO into thinking you have. Thus,it disconnects him and resets the equipment to prepare for the next call. All this happens very quickly (300-800ms for step-by-step equipment and 150-400ms for other equipment).

When you stop sending 2600Hz (after about a second), the equipment thinks that another call is coming towards it (e.g. it thinks the far end has come "off-hook" since the tone has stopped. It could be thought of as a toggle switch: tone --> on hook, no tone -->off hook. Now that you've stopped sending 2600Hz, several things happen:

1) A trunk is seized.

2) A "wink" is sent to the CALLING end from the CALLED end indicating that the CALLED end (trunk) is not ready to receive digits yet.

3) A register is found and attached to the CALLED end of the trunk within about two seconds (max).

4) A start-dial signal is sent to the CALLING end from the CALLED end indicating that the CALLED end is ready to receive digits.

Now, all of this is pretty much transparent to the blue boxer. All he really hears when these four things happen is a <beep><kerchunk>. So, seizure of a trunk would go something like this:

1) Send a 2600Hz

2) Terminate 2600Hz after 1-2 secs.

3) [beep][kerchunk]

Once this happens, you are connected to a tandem that is ready to obey your every command. The next step is to send signalling information in order to place your call. For this you must simulate the signalling used by operators and automatic toll-dialing equipment for use on trunks. There are mainly two systems, DP and MF. However, DP went out with the dinosaur , so I'll only discuss MF signalling. MF (multi-frequency) signalling is the signalling used by the majority of the inter- and intra-lata network. It is also used in international dialing known as the CCITT no.5 system.

MF signalling consists of 7 frequencies, beginning with 700Hz and separated by 200Hz. A different set of two of the 7 frequencies represent the digits 0 thru 9, plus an additional 5 special keys. The frequencies and uses are as follows:

Frequencies (Hz)	Domestic	Int'l
700 + 900	1	1
700 + 1100	2	2
900 + 1100	3	3
700 + 1300	4	4
900 + 1300	5	5
1100 + 1300	6	6
700 + 1500	7	7
900 + 1500	8	8
1100 + 1500	9	9
1300 + 1500	0	0
700 + 1700	ST3p	Code 11
900 + 1700	STp	Code 12
1100 + 1700	KP	KP1
1300 + 1700	ST2p	KP2
1500 + 1700	ST	ST

The timing of all the MF signals is a nominal 60ms, except for KP, which should have a duration of 100ms. There should also be a 60ms silent period between digits. This is very flexible, however, and most Bell equipment will accept outrageous timings.

In addition to the standard uses listed above, MF pulsing also has expanded usages known as "expanded inband signalling" that include such things as coin collect, coin return, ringback, operator attached, and operator released. KP2, code 11, and code 12 and the ST_ps (STart "primes") all have special uses which will be mentioned only briefly here.

To complete a call using a blue box, once seizure of a trunk has been accomplished by sending 2600Hz and pausing for the <beep><kerchunk>, one must first send a KP. This readies the register for the digits that follow. For a standard domestic call, the KP would be followed by either 7 digits (if the call were in the same NPA as the seized trunk) or 10 digits (if the call were not in the same NPA as the seized trunk). [Exactly like dialing a normal fone call]. Following either the KP and 7 or 10 digits, a STart is sent to signify that no more digits follow. Example of a complete call:

1) Dial 1-806-258-1234

2) wait for a call-progress indication
(such as ring, busy, recording, etc.)

3) Send 2600Hz for about 1 second.

4) Wait for about 2 seconds while a trunk is seized.

5) Send KP+305+994+9966+ST

The call will then connect if every-thing was done properly. Note that if a call to an 806 number were being placed in the same situation, the area code would be omitted and only KP+ seven digits+ST would be sent.

Code 11 and code 12 are used in international calling to request certain types of operators. KP2 is used in international calling to route a call other than by way of the normal route, whether for economic or equipment reasons.

STp, ST2p, and ST3p (prime, two prime, and three prime) are used in TSPS signalling to indicate calling type of call (such as coin-direct dialed).

This has been Part I of Better Homes and Blue Boxing. I hope you enjoyed and learned from it. If you have any questions, comments, threats or insults, please fell free to drop me a line. If you have noticed any errors in this text (yes, it does happen), please let me know and perhaps a correction will be in order. Part II will deal mainly with more advanced principles of blue boxing, as well as routings and operators.

Note 1 other highly trunkable areas include:
816,305,813,609,205. I personally have excellent luck boxing off of 609-953-0000. Try that if you have any trouble.

Better Homes and Blue Boxing
Part II: Practical Applications

(It is assumed that the reader has read and understood Part I of this series).

The essential purpose of blue boxing in the beginning was merely to receive toll services free of charge. Though this can still be done, blue boxing has essentially outlived its usefulness in this area. Modern day "extenders" and long distance services provide a safer and easier way to make free fone calls. However, you can do things with a blue box that just can't be done with anything else. For ordinary toll-fraud, a blue box is impractical for the following reasons:

1) Clumsy equipment required (blue box or equivalent)

2) Most boxed calls must be made through an extender. Not for safety reasons, but for reasons I'll explain later.

3) Connections are often sacrificed because considerable distances must be dialed to cross a seizable trunk, in addition to awkward routing.

As stated in reason #2, boxed calls are usually made through an extender. This is for billing reasons. If you recall from Part I, 2600Hz is used as a "supervisory" signal. That is, it signals the status of a trunk--"on-hook" or "off-hook." When you seize a trunk (by briefly sending 2600Hz), your end (the CALLING end) goes on hook for the duration of the 2600Hz and then goes off-hook once again when the 2600Hz is terminated. The CALLED end recognizes that a call is on the way and attaches a register, which interprets the digits which are to be sent. Now, understand that even though your end has come off-hook (no 2600Hz present), the other end is still on-hook. You may wonder then, why, if the other end (the CALLED end) is still on-hook, there is no 2600Hz coming the other way on the trunk, when there should be. This is correct. 2600Hz *IS* present on the trunk when you seize it and afterwards, but you cannot hear it because of a Band Elimination Filter (BEF) at your central office.

Back to the problem. Remember that when you seize a trunk, 2600Hz is indeed coming the other way on the trunk because the CALLED end is still on-hook, but you don't actually hear it because of a filter. However, the Bell equipment knows it's there (they can "hear" it). The presence of the 2600Hz is telling the billing equipment that your call has not yet been completed (i.e., the CALLED end is still on-hook). When finally you do connect with your boxed call, the 2600Hz from the called end terminates. This tells the billing equipment that someone picked up the fone at the CALLED end and you should begin to be billed. So you do start to get billed, but for the call to the trunk, NOT the boxed call. Your billing equipment thinks that you've connected with the number you used to seize the trunk. Illustration:

1) You call 1+806-258-2222 (directly)

2) Status of trunks:

```
          <-------------------------------------->
          (You) --------------------- 806-258-2222
          No 2600Hz ---------><------------ 2600Hz
```

When you seize a trunk (before the number you called answers) there is no affect on your billing equipment. It simply thinks that you're still waiting for the call to complete (the CALLED end is still on-hook; it is ringing, busy, going to recorder or intercept operator.

Now, let's say that you've seized a trunk (806-258-2222) and for example, KP+314+949+1705+ST. The call is routed from the tandem you seized to: 314-949-1705.

Illustration:

```
          <------------------>O<----------------->
          (You) ------------ 806 --------- 314-949

                           tandem

          No 2600Hz --------- >< ---------- 2600Hz
```

Note that the entire path towards the right (the CALLED end) has no 2600Hz present and is therefore "off-hook." The entire path towards the left (the CALLING end) does have 2600Hz present on it, indicating that the CALLED end has not picked up (or come "off-hook"). When 314-949-1705 answers, "answer supervision" is given and the 2600Hz towards the left (the CALLING end) terminates. This tells your billing equipment, which thinks that you're still waiting to be connected with 806-258-2222, that you've finally connected. Billing then begins to 806-258-2222. Not exactly an auspicious beginning for an aspiring young phone phreak.

To avoid this, several actions may be taken. As previously mentioned, one may avoid being charged for the number called to seize a trunk by using an extender (in which case the extender will get billed). In some areas, boxing may be accomplished using an 800 number, generally in the format of 800-858-xxxx (many Amarillo numbers) or 800-NN2-xxxx (special intra-state class in-WATS numbers). However, boxing off of 800 numbers is impossible in many areas. In my area, Denver, I am served by #1A ESS and it is impossible for me to box off of any 800 number.

Years ago, in the early days of blue boxing (before my time), phreaks often used directory assistance to box off of because they were "free" long distance calls. However, because of competitive long distance companies, directory assistance surcharges are now $0.50 in many areas. It is additionally advised that directory assistance numbers not be used to box from because of the following:

- Average DA calls last under 2 minutes. When you box a call, chances are that it will last considerably longer. Thus, the Bell billing equipment will make a note of calls to directory assistance that last a long time. A call to a directory assistant lasting for 4 hours and 17 minutes may appear somewhat suspicious.

- Although the date, time, and length of a DA call do not appear on the bill, it is recorded on AMA tape and will trip a trouble report if it were to last too long. This is how most phreaks were discovered in the old days. Also, sometimes too many calls lasting too long to one 800 number may raise a few eyebrows at the local security office.

Assuming you can complete a blue box call, the following are listed routings for various Bell internal operators. These are in the format of KP+NPA+ special routing+1X1+ST, which I will explain later. The 1X1 is the actual operator routing, and NPA and NPA+ special routing are used for out-of-area code calls and out-of-area code calls requiring special routing, respectively.

KP+101+ST Toll test board.

KP+121+ST Inward Operator.

KP+131+ST Directory assistance.

KP+141+ST was rate & route. Now only works in 312, 815, 717, and a few others. It has been replaced with a universal rate & route number 800+141+1212.

KP+151+ST Overseas completion operator (inbound). Works only in certain NPAs, such as 303.

KP+181+ST In some areas, toll station for small towns.

Thus, if you seize a trunk in 806 NPA and wanted an inward (in 806), then you would dial KP+121+ST. If you wanted a 312 inward and were dialing on an 806 trunk, an area code would be required. Thus, you would dial KP+312+121+ST. Finally, some places in the network require special routing, in addition to an area code. An example is Franklin Park, Ill. It requires a special routing of 032. For this, you would dial KP+312+032+121+ST for a Franklin Park inward operator.

Special routings are in the format of 0XX. They are used primarily for load balance, so that traffic flow may be evenly distributed. About half of the exchanges in the network require special routing. Note that special routings are NEVER EVER EVER used to dial normal telephone numbers, only operators.

Operator functions

Toll Test Board

Generally a cordboard position that assists in trunk testing. They are not used by operators, only switchmen.

Inward

Assists the normal TSPS (0+) operator in completing calls out of the TSPS's area. Also, inwards perform emergency interrupts when the number to be interrupted is out of the area code of the original (TSPS) operator. For example, a 303 operator has a customer that needs an emergency interrupt on 215-647-6969. The 303 operator gets the routing for the inward that covers 215-647, since she cannot do the interrupt herself. The routing is found to be only 215+ (no special routing required). So, the 303 operator keys KP+215+121+ST. An inward answers and the 303 says to her, "Inward, this is Denver. I need an emergency interrupt on 215-647-6969. My customer's name is Mark Tabas." The inward will then do the interrupt (off the line, of course). If the number to be interrupted had required special routing, such as, say, 312-456-1234 (spec routing 032), then the 303 operator would dial

KP+312+032+121+ST for the inward to do that interrupt.

Directory Assistance
These are the normal NPA+555+1212 operators that assist customers with obtaining telefone directory listings. Not much toll-fraud potential here, except maybe $0.50.

Rate and Route
These operators are reached by dialing KP+800+141+1212+ST. They assist normal (TSPS) operators with rates and routings (thus the name). The only uses I typically have for them are the following:

1. Routing-Information
   In the above example, when the 303 operator needed to dial an inward that served 215-647, she needed to know if any special routing was required and, if so, what it was. Assuming she would use rate and route, she would dial them and say nicely, "Operator's route, please, for 215-647." Rate & route would respond with "215 plus." This means that the operator would dial KP+215+121+ST to reach the inward that serves 215-647. If there were special routing required, such as in 312-456, rate & route would respond with "312 plus 032 plus." In that case, the operator would dial KP+312+032+ST for the inward that serves 312-456.

   It is good practice to ask for "operator's route" specifically, as there are also "numbers route" and "directory routes." If you do not specifically ask for operator's route, rate & route will generally assume that is what you want anyway.

   "Numbers" route refers to overseas calls. Example, you want to know how to reach a number in Geneva, Switzerland (and you already have the number). You would call routing and say "Numbers route, please, Geneva, Switzerland." The operator would respond with: "Mark 41+22. 011+041+ST (plus) 041+22" The "Mark 41+22" has to do with billing, so disregard it. The 011+041 is access to the overseas gateway (to be discussed in Part III) and the 041+ 22+ is the routing for Geneva from the overseas sender.

"Directory" routings are for directory assistance overseas. Example: you want a DA in Rome, Italy. You would call rate & route and say, "Directory routing please, for Rome, Italy." They would respond with "011+039+ST (plus) 039+1108 STart." As in the previous example, the 011+039 is access to the overseas gateway. The 039+1108 is a directory assistant in Rome.

2. Nameplace information
Rate & Route will give you the location of an NPA+ exchange. Example: "Nameplace please, for 215-648." The operator would respond with "Paoli, Pennsylvania." This isn't especially useful, since you can get the same information (legally) by dialing 0, but using rate & route is often much faster and it avoids having to hang up when you are already on a trunk.

Note On Rate & Route: As a blue boxer, always ask for "IOTC" routings. (e.g., "IOTC operator's route", "IOTC numbers route", etc.) This tells them that you want cordboard-type routings, not TSPS, because a blue boxer is actually just a cordboard position (that Bell doesn't know about).

Overseas Completion

1. Operator (inbound)
These operators (KP+151+ST) assist in the completion of calls coming in to the United States from overseas. There are KP+151+ST operators only in a few NPAs in the country (namely 303). To use one, you would seize a trunk and dial KP+303+151+ST. Then you would tell the operator, for example, "This is Bangladesh calling. I need U.S. number 215-561-0562 please." [in a broken Indian accent]. She would connect you, and the bill would be sent to

Bangladesh (where I've been billing my KP+151+ST calls for two years).

2. Other internal Bell Operators.

KP+11501+ST	universal operator
KP+11511+ST	conference operator
KP+11521+ST	mobile operator
KP+11531+ST	marine operator
KP+11541+ST	long distance terminal
KP+11551+ST	time & charges operator
KP+11561+ST	hotel/motel operator
KP+11571+ST	overseas (outbound) operator

These 115X1 operators are identical in routing to the 1X1 operators listed previously, with one exception. If special routing is required (0XX), then the trailing 1 is left off.

Examples

A 312 universal op ... KP+312+11501+ST.
A Franklin Park (312-456) universal op (special routing 032 required).
KP+312+032+1150+ST (The trailing 1 of 11501 is left off).

Purposes of 115X1 operators

Universal Used for collect/callback calls to coin stations.

Conference This is a cordboard conference operator who will set up a conference for a customer on a manual operation basis.

Mobile Assists in completion of calls to mobile (IMTS) type telefones.

Marine Assists in completion of calls to ocean going vessels.

Long Distance Terminal   Now obsolete.Was used for completion of long distance calls.

Time & Charges   Will give exact costs of calls. Used to time calls and inform customer of exactly how much it cost.

Hotel/Motel   Handles calls to/from hotels and motels.

3. Overseas Completion (outbound)
Assists in completion of calls to overseas points. Only works in some, if any NPAs, because overseas assistance has been centralized to IOCC (covered in Part III).

Note that all KP+1X1+ST and KP+115X1+ST operators automatically assume that you are a TSPS or cordboard operator assisting a customer with a call. Do not do anything to jeopardize this! If you do not know what to do, don't call these operators! Find out what to do first.

This concludes Part II. There is one final part in which I will explain overseas dialing, IOCC (International Overseas Completion Centre), RQS (Rate/Quote System), and some basic scanning.

Better Homes and Blue Boxing
Part III: Advanced Signalling

(It is assumed that the reader has read and understood parts I

& II before proceeding to this part).

In Parts I & II, I covered basic theory and domestic signalling and operators. In this part I will explain overseas direct boxing, the IOCC, the RQS, and some basic scanning methods.

Overseas Direct Boxing

Calling outside of the United States and Canada is accomplished by using an "overseas gateway." There are 7 overseas gateways in the Bell System, and each one is designated to serve a certain region of the world. To initiate an overseas call, one must first access the gateway that the call is to be sent on. To do this automatically, decide which country you are calling and find its country code. Then, pad it to the left with zeros as required so it is three digits. [Add 1, 2, or 3 zeros as required].

Examples

Luxembourg (352) is 352 (stays the same)
Spain (34) becomes 034 (1 zero added)
U.S.S.R. (7) becomes 007 (2 zeros added)

Next, seize a trunk and dial KP+011+ CC+ST. Note that CC is the three digit padded country code that you just determined by the above method. [For Luxembourg, dial KP+011+352+ST, Spain KP+011+034+ST, and the U.S.S.R. KP+011+007+ST]. This is done to route you to the appropriate overseas gateway that handles the country you are dialing. Even though every gateway will allow you to dial every dialable country, it is good practice to use the gateway that is designated for the country you are calling.

After dialing KP+011+CC+ST (as CC is defined above) you should be connected to an overseas gateway. It will acknowledge by sending a wink (which is audible as a <beep><kerchink> and a dial tone. Once you receive international dial tone, you may route your call one of two ways: a) as an operator-originated call, or b) as a customer-originated call. To go as a operator-originated call, key KP+ country code (NOT padded with zeros)+ city code+number+ST. You will then be connected, providing the country you are calling can receive direct-dialed calls. The U.S.S.R. is an example of a country that cannot.

Example of a Boxed International Call

To make a call to the Pope (Rome, Italy), first obtain the country code, which is 39. Pad it with zeros so that it is 039. Seize a trunk and dial KP+011+039+ST. Wait for sender dial tone and then dial KP+39+6+6982+ST. 39 is the country code, 6 is the city code, and 6982 is the Pope's number in Rome. To go as an operator-originated call, simply place a zero in front of the country code when dialing on the gateway. Thus, KP+0+39+6+6982+ST would be dialed at sender dial tone. Routing your call as operator-originated does not affect much unless you are dialing an operator in a foreign country

To dial an operator in a foreign country, you must first obtain the operator routing from rate & route for that country. Dial rate & route and if you're trying to get an operator in Yugoslavia, say nicely, "IOTC Operator's route, please, for Yugoslavia." [In larger countries it may be necessary to specify a city]. Rate & route will respond with, "38 plus 11029". So, dial your overseas gateway, KP+011+038+ST, wait for sender dial tone, and key KP+0+38+11029+ST. You should then get an operator in Yugoslavia. Note that you must prefix the country code on the sender with a 0 because presumably only an operator here can dial an operator in a foreign country.

When you dial KP+011+CC+ST for an overseas gateway, it is translated to a 3-digit sender code of the format 18X, depending on which sender is designated to handle the country you are dialing. The overseas gateways and their 3-digit codes are listed below.

182	White Plains, NY
183	New York, NY
184	Pittsburg, PA
185	Orlando, FL
186	Oakland, CA
187	Denver, CO
188	New York, NY

Dialing KP+182+ST would get you the sender in White Plains, and KP+183+ST would get the sender in NYC, etc., but the KP+011+CC+ST is highly suggested (as previously mentioned). To find out what sender you were routed to after dialing KP+011+CC+ST, dial (at int'l dial tone): KP+0000000+ST.

If you have difficulty in reaching a sender, call rate and route and ask for a numbers route for the country you're dialing. Sometimes, KP+011+ padded country code+ST will not work. I have found this in many 3-digit country codes. Luxembourg, country code 352, for example, should be KP+011+352+ST theoretically. But it is not. In this case, dial KP+011+ 003+ST for the overseas gateway. If you have trouble, try dialing KP+00+ first digit of country code+ST, or call rate The IOCC.

Sometimes when you call rate and route and ask for an "IOTC numbers route" or "IOTC operators route" for a foreign country, you will get something like "160+700" (as in the case of the Soviet Union). This means that the country is not dialable directly and must be handled through the International Overseas Completion Centre (IOCC). For an IOCC routing, pad the country code to the RIGHT with zeros until it is 3 digits. Then KP+160 is dialed, plus the padded country code, plus ST.

Examples:

The U.S.S.R. (7)	KP+160+700+ST
Japan (81)	KP+160+810+ST
Uraguay (598)	KP+160+598+ST

You will then be routed to the IOCC in Pittsburg, PA, who will ask for country, city, and number being dialed. Many times they will ask for a ringback (thanks to Telenet Bob) so have a loop ready. They will then place the call and call you back (or sometimes put you through directly). Some calls, such as to Moscow, take several hours.

The Rate Quote System (RQS)

The RQS is the operator's rate/quote system. It is a computer used by TSPS (0+) operators to get rate and route information without having to dial the rate and route operator. In Part II, I discussed getting an inward routing for dialing-assistance and emergency interrupts from the rate and route operators (KP+800+141+1212+ST). The same information is available from RQS. Say you want the inward routing for 305-994. You would seize a trunk and dial KP+009+ST (to access the RQS). Sometimes, if you seize a trunk in an NPA not equipped with RQS, you need to dial an NPA that is equipped with RQS first, such as 303. Anyway, after you dial KP+009+ST or KP+303+009+ST, you will receive a wink (<beep><kerchink>) and then RQS dial tone. At RQS dial tone, for an inward routing for 305-994 you would dial KP+06+305+994+ST. That is, KP+06+NPA+exchange+ST. RQS will respond with "305 plus 033 plus". This means you would dial KP+305+033+121+ST for an inward that services 305-994. If no special routing were required, RQS would have responded with "305 plus" and you would simply dial: KP+305+121+ST for an inward.

Another RQS feature is the echo feature. You can use it to test your blue box. Dial RQS (KP+009+ST) and then key KP+07+1234567890+ST. RQS will respond with voice identification of the digits it recognized, between the KP+07 and ST.

RQS can also be used for rates and directory routings, but those are seldom needed, so they have been omitted here.

Simple Scanning

If you're interested in scanning, try dialing on a trunk, routings in the format of KP+11XX1+ST. Begin with 11001 and scan to 11991. There are lots of interesting things to be found there, as Doctor Who (413 area) can tell you. Those 11XX1 routings can also be prefixed with an NPA, so if you want to scan area code 212, dial KP+212+ 11XX1+ST.

There, now you know as much about blue boxing as most phreaks. If you read and understand the material, and put aside preconceived ideas of what blue boxing is that you may have acquired from inexperienced people or other bulletin boards, you should be well on you way to an enlightening career in blue boxing. If you follow the guidelines in Part I to box, you should have no problem with the fone company. Comments made by "phreaks" on bulletin boards that proclaim "tracing" of blue boxers are nonsense and should be ignored (except for a passing chuckle).

Note 1: CCIS and the Downfall of Blue Boxing

CCIS stands for Common Channel Inter-office Signalling. It is a signalling method used between electronic switching systems that eminiates the use of 2600Hz and 3700Hz supervisory signals, and MF pulsing. This is why many places cannot be boxed off of; they employ CCIS, or out-of-band signalling, which will not respond to any tones that you generate on the line. Eventually, all existing toll equipment will be upgraded or replaced with CCIS or T-carrier. In this case, we'll all be boxing with microwave dishes. Until then (about 1995 by current BOC/AT&T estimates), have fun!

If you have ANY questions about this text, please feel free to drop me a line. I will respond to all mail, messages, etc. Insults are also welcomed. And if you discover anything interesting scanning, be sure to let me know.

Mark Tabas
LOD

This text was prepared in full by Mark Tabas for:

K.A.O.S.
Philadelphia, PA.
[215-465-3593].

Technical acknowledgements

Karl Marx, X-Man, High-Rise Joe, Telenet Bob, Lex Luthor, TUC, John Doe, Doctor Who (413 area), The Tone Sweep, Mr. Silicon, K00L KAT, The Glump.

References

1. Notes on the BOC Intra-LATA Networks Bell System publication, 1983.

2. Notes on the Network Bell System publication, 1983.

3. Engineering and Operations in the Bell System Bell System publication, 1983.

4. Notes on Distance Dialing Bell System publication, 1968.

5. Early Medieval Architecture.

By Fred Steinbeck (TAP #88)

It seems that fewer and fewer people have blue boxes these days, and that is really too bad. Blue boxes, while not all that great for making free calls (since the tpc can tell when the call was made, as well as where it was too 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 the rate & route (R&R) operators. To get the R&R op, you send a KP + 141 + ST. In some areas you may need to put another NPA before the 141 (i.e., KP + 213 + 141 + ST), if you have no local R&R ops.

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

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

Sometimes directory assistance isn't just NPA + 131. The way to get these routings is to call R&R and ask for "Anaheim, California, directory route, please." of course, she'd tell us it was 714 plus, which means 714 + 131 gets us the D.A. op there. This is sort of 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 say, "916 plus 001 plus." this means that 916 + 001 + 121 will get you the inward operator for Sacramento.

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

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

Inward operator routings to various countries are obtained the same way "International, London, england, tsps inward route, please." and get "Country code 44 plus 121." therefore, 44 plus 121 gets you inward for London.

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

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

Note as a result of the break-up, R&R is now
     KP+800+141+1212+ST

Verification

From TAP issue # 88, 10-83

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

Needless to say, Bell System is very tight lipped about knowledge regarding verification. Indeed, the infamous book 'Notes on long distance dialing' ('68 edition) says, "Care must be taken to insure that the customer never gains verification capabilities." With a printed policy like that, you can imagine what their real-world policy is like! Even their own rate and route operators will not give verification on 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 TAPer on the right track, and perhaps he or she will show us all how. If you have knowledge not covered in this article, but don't want to write an article on your own, please send your ideas, comments, or information to Project Verify, C/O TAP Verify has also been called "Autoverify", and I have no idea why. This is not, to my knowledge, a Bell System term (at least I've never seen it in any manuals) As far as I know, there is verify, which means being able to listen to speech (kind of; see below) on a line, and there is the "Emergency Interrupt which allows you to take part in the conversation taking place on the line in question. It has been suggested that "Autoverify" is the same as an emergency interrupt , but I tend to disagree with this idea. It should be noted that the verification circuitry does not actually let an operator listen to a conversation without making a beep on the line every so often. Instead, she will hear encrypted speech. However, I believe with the proper methods, verify can be converted to an emergency interrupt.

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

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

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

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

The verification circuit, as you know, likes to encrypt conversation, which is something we don't want. Well, the second Ring FWD sends another 90 volts crashing against the verify circuitry, which Juda 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 as "VFY BY", or verify busy for the 213 NPA. 002 is listed for the 805 NPA. Ma Bell likes to have standardized routing codes, such 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, 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 the tend to give information out easier if you ask for something that you would ordinarily have to be a company employee to know about, such as rate steps, operator routings, etc.

Casually let slip that you used to be (or still are) an operator, or that you work for company security. Also, you might want to blue box some codes like 001 followed by your NPA and the last 7D of a busy number. If you get a sort of "whispery noise", try blasting the line with a ringing signal (you might piggyback another line onto yours and call the piggyback to generate the 90 volts) and see if that does anything.

Equal Access and the American Dream

By Mark Tabas
P.O. Box 620401
Littleton, CO 80162

July 7, 1985

The American Dream means many things to many people. To the small, typical businessman, it means building a good, strong business based on hard work and perseverance; indeed, with nothing limiting his potential but he amount of work he is willing to put into his business. To a large businessman, the American Dream means living and working in a country where a single corporation can have a profit exceeding the gross national product of an entire third world nation.

To the individual, the American Dream is the right to choose -- everything from one's breakfast cereal to a long-distance service, as well as the formal right outlined by our founding fathers: those of life, liberty, and the pursuit of happiness.

To the phone phreak, I think the American Dream is, in a sort of twisted way, the uninhibited pursuit of knowledge. This quest could scarcely remain unchecked in many other countries. Analogous to this quest is the thriving of the Bell System, which until January 1, 1984 consisted of the American Telephone and Telegraph Company, the largest corporation in the history of the world. Did the American Dream die on January first or did the divestiture of AT&T cause a giant step forward for competition and free enterprise in the United States? I do not know. I do know that the other nations of the world were amazed that the United States would dissolve the entity that brought the finest and most universal telephone system in the world, and did so at a time when the majority of the rest of the world was still using two dixie cups and a string.

The unfairness of the situation is that AT&T built the telephone system of this nation and is now being bound and gagged and having its possessions distributed to others, whom AT&T also wrought. All in the name of fairness, free competition, and "equal access". Where was was MCI during the century that AT&T built he communications system of this nation? Well, I believe in Equal Access, Wholly. And, since I believe in equal access and its implications for equality for all so strongly, I feel that MCI, Sprint, and others should take the same amount of time to build their respective toll networks: 100 years. Therefore, if the United States Justice Department were truly the fair and just administrator that it portrays itself to be, MCI would not have a hand in the long-distance cache until about 2080. That's only fair.

There is no doubt that MCI is a sub-standard organization. They consist of incompetent employees, inferior equipment, and an inferior marketing strategy. They are mockingly imitative of AT&T, except in the quality of their service, which is practically unusable. It is also interesting that with less than 2% market share, MCI calls itself "the nation's long-distance company." The point to this diatribe is this. It's time for these long-distance companies such as MCI and Sprint to grow up. With Equal Access, they are going to become real long-distance companies, not the joke organizations they are now, and I think it may just take them one hundred years to do so.

Equal Access

Equal Access, as it applies to the telecommunications industry, is "the requirement that each Bell Operating Company provide exchange access to all long-distance carriers that is equal in type and quality to that provided AT&T communications." This is the official provision set forth by the United States Justice Department in the Modification of the Final Judgment, August 24, 1982. All this means is that each long-distance-distance company will have "equal access" to all of the same types of services that AT&T currently enjoys. There are four types of long-distance carrier services, divided into "feature groups." They follow.

FG A "line side access." This is the standard 7-digit dialup+code (for billing purposes) +destination telephone number. It is currently in use by most long-distance carriers.

FG B "trunk side access." These are the 950 exchange numbers. They also utilize an authorization code for billing. As with FG A, automatic number identification (ANI) (i.e. calling number) is not provided to the carrier, but will be in the future.

FG C "1+ dialing." Currently, only AT&T is able to get this type of service. It is 1/0+7 of 10 digit direct long distance dialing. ANI (for billing) is provided.

FG D "equal access." This will allow for 1/0+7 or 10 digit direct long-distance dialing (presubscription carrier) and 10xxx+1/0+7 or 10 digit long-distance dialing (alternate carrier). ANI for billing is provided at the long-distance carrier's option. Billing may also be handled by the individual long distance company or the local Bell Operating Company.

Feature groups C and D are mutually exclusive (i.e. both cannot exist in a particular area at the same time). Areas which have Feature Group C (AT&T long-distance only) are non-Equal Access, and areas which have Feature Group D (multiple long distance carriers) are Equal Access regions.

Feature Group B, the 950 exchange numbers will be used in areas in which it is not feasible to provide with Equal Access, such as step-by-step offices (yes, they CAN have 950 numbers), some crossbar offices, and some independent telcos, which are not bound by the provisions of Equal Access and may provide to their customers any type of long-distance service(s) they wish. The 950 exchange is now active in many areas. It is mainly used as a universal "roaming" access port for many long-distance carriers, but when an office is converted to Equal Access, the 950 capability is removed. Thus, in an Equal Access region, one cannot complete a call to a 950 telephone number.

I personally am looking very forward to Equal Access. My area is not scheduled for full implementation of it until late 1985 or early 1986, and by this time many of the alternate long distance carriers' networks will be in place (or well under way). Think about what Equal Access means. Equality for all long distance carriers. Access to common facilities, such as: busy-line verification lines, Bell System information, signalling specifications. etc. After full implementation of Equal Access, one will be able to take advantage of and manipulate the services of more than just one carrier. It will no longer be phreaks vs. AT&T.

When your area is ready to initiate Equal Access, you will receive a notice in the mail informing you of some of the details of Equal Access, and will ask you to specify your choice of "primary carrier." In some cases you will need to specify both inter-LATA carrier (IC), which handles calls out of your LATA (Local Access and Transport Area), and an international carrier (INC), which will handle calls destined for other countries. Recent market studies have shown that between 80 and 90 per cent of residential customers will continue to be served by AT&T for their long-distance service after Equal Access. So much for competition.

You will probably be faced with many long-distance companies to choose from, including but not limited to: AT&T, MCI, Sprint, ITT, Western Union, Dial U.S., Call America, TMC, and U.S. Telephone. Whichever you choose will become your "primary carrier." Your primary carrier will handle your call each time you pick up you fone and dial 1+7 or 10 digits or 0+7 or 10 digits, inter-LATA only. That is, if you dial a toll call that is within your LATA, it will be handled by your local telephone company (Bell), not by your primary carrier, even though it is a toll call. Let's use an example. The state of Colorado consists of two LATAs. For this example, I will use three cities in Colorado:

- Denver (in LATA1)
- Sterling (LATA1 also)
- Colorado Springs (in LATA2).

Note here that even though Denver ad Sterling are in the same LATA, and Denver and Colorado Springs are not, Sterling is actually much farther away from Denver than Colorado Springs. This is because LATA boundaries were designed giving consideration to high toll-traffic regions, to bring in revenue. Toll traffic between Denver and Colorado Springs is very high, so the two cities were placed in separate LATAs (or, more correctly, they were separated by a LATA boundary).

Toll traffic between Denver and Sterling is very low, of the two cities were allowed to remain in the same LATA. Now, if everyone in Colorado Springs were to pack up and move to Sterling (though who knows what the hell for), the LATA boundaries in Colorado would be changed so that Denver and Sterling were in different LATAs. The primary factor in determining LATAs is money.

If I made a call to Sterling from my home in Denver, the call would be routed entirely via Mountain Bell long-distance facilities. No long distance carrier would be involved because Denver and Sterling are in LATA1. If I made a call to Kelley, the blonde babe in Colorado Springs, the call would be handled by a long distance carrier (in this case, AT&T) because Denver is in LATA1 and Colorado Springs is in LATA2. Here is a table to simplify this:

Customer dials	LATA	Carrier
7 digits	same	Bell
1+7 digits	same	Bell
1+7 digits	diff	LD carrier (currently AT&T)
1+10 digits	diff	LD carrier (currently AT&T)

Note several things here. First, not all areas need to dial a 1 when dialing any number, local or long distance, but the central offices will still discern whether the call is in the same LATA as the customer or a different one and handle the call appropriately. Secondly, some step-by-step offices require a 1+NPA to be dialed for calls within the same LATA and, in fact, all numbers outside of the office itself. But, for the most part, the above table is standard for common switching networks.

Alternate Carriers

Your normal long distance carrier will handle all your toll calls which cross over LATA boundaries when you dial directly, 1+. If you wish to place your call via another carrier's network, whether for cost, quality, or circuit availability reasons, you may do so in Equal Access regions. To access an alternate long distance carrier after Equal Access, a customer dials 10xxx+1/0+7 or 10 digit telefone number. Note that xxx is the "carrier access code (CAC)." A few CACs currently in use are listed below.

220	Western Union	666	Lexitel
222	MCI	777	Sprint
333	US Telefone	888	SBS
444	Allnet		

Thus, in an Equal Access region, to dial Fred in Orlando, a customer would dial 1+305+994+9966 to place his call on his primary carrier, or to place it on another network, he could dial: 10222+1+305+994+9966, and the call would go over MCI facilities (in this case). Eventually, after many more long distance services get into the act, there will be a directory of the various long distance companies and their CACs, and deciding which carrier to use for any particular call to get the bet rate will be beyond the ability of everyone except phone phreaks.

<<> G-File: The Official Phreakers Manual: PHREAK*.DOC   203
     G_PHREAK.WPS 11/20/90 11:29 AM

The 950 Exchange

As discussed, the 950 central office exchange is currently a "roaming" access port for various long distance carriers. In areas that have 950, the access to carriers is standardized. Thus, someone travelling to several different areas need only know the 950 number of the carrier he uses to access it from any area (provided that it have 950 active). Originally, the 950 exchange was designed to correspond with the 10xx carrier access code used for Equal Access. For example, 950-1022 would be the same carrier as 1022 (+telephone number). However, it was later found that the 100 codes available for use as 10xx CACs would be insufficient to handle he number of long distance carriers. So, the common carrier access code was increased by one digit, to 10xxx, thus increasing the number of possible CACs to 1000. To keep the 950 exchange consistent with the non CAC, the Bell Operating Companies have opted to change the 950-10xx to 950-0xxx. The xxx in the 950-0xxx remains the same as the xxx in the 10xxx carrier access code. The new modified 950 numbering pan is now active in Philadelphia (Bell Atlantic) among other areas.

After Equal Access is well under way, the 950 exchange will be used in certain areas that cannot be equipped for the standard Equal Access dialing plans. This includes step-by-step, #1 crossbar, #5 crossbar, #2ESS, and #3ESS offices. Customers in areas served by these types of switching equipment will dial 950-0xxx, wait for acknowledgement tone from the carrier, and then dial a "personal identification number" and destination telefone number,and the call will be completed on the selected carrier's facilities. Initially, billing will be handled by the carrier itself, and supervisory information and ANI will not be provided by the local Bell Operating Company.

There are three main advantages to the 950 central office exchange and protocol. They are:

a) universal access for all areas

b) 950-exchange numbers are "trunk side access." This means that the long distance carrier has direct trunks going to it from a Bell toll office or local central office. These trunks are interoffice lines, not customer type (POTS) lines, and supposedly insure higher quality of connection.

c) 950-exchange numbers are toll and message unit free. On metered-usage (i.e., not "flat rate") customer lines, they cost nothing. In most areas they are free from coin stations, with Colorado as one notable exception.

Costs

Each long-distance carrier must choose the type(s) of service it wishes to provide to its customers. These different types of service were outlined earlier as "Feature Groups." The costs of these Feature Groups vary directly with the complexity and quality of the service itself. The following table outlines the cost to the carrier of each available Feature Group. It is based on the monthly rate per line for 9000 minutes of circuit use, and assumes the carrier and Bell switch are 15 miles apart.

FG	non-Equal Access	Equal Access
A	$329.94	$709.20
B	329.94	721.80
C	752.40	N/A
D	N/A	752.40

These figures are a lot more significant than they might appear. They indicate that after Equal Access, in order to compete with the giants such as AT&T, MCI, etc., smaller long distance companies will use Feature Group A or B type service in order to provide significantly lower rates to their customers than companies subscribing to Feature Group D service (like AT&T, MCI, etc). This will cause a unique type of equilibrium to form. Customers willing to dial an access number, authorization code, and destination number and put up with lower quality service will be able to save a lot of money. This seems faintly reminiscent of pre-Equal Access times....

Directory Assistance

Each Bell Operating Company will be responsible for providing intra-LATA operator services. When a customer dials (1)+411 or (1)+555+1212 for local directory assistance, he will reach a Bell operator who will service requests for listed numbers within the customer's LATA. Requests for numbers in LATAs other than the calling customer's may be handled at the discretion of the local operating company. Initially, the Bell Operating Companies will meet the responsibility for providing directory assistance services by contracting it to a long distance carrier or carriers (currently AT&T). All inter-LATA directory assistance services will be provided by the inter-LATA carrier (IC). ICs may also provide 800 Enterprise service or other toll free type directory assistance services. See table.

Intra-LATA

HNPA	411/555-1212	BOC
*FNPA	NPA+555-1212	BOC
HNPA	10xxx+555-1212	intra-LATA carrier
*FNPA	10xxx+NPA+555-1212	intra-LATA carrier

Inter-LATA

HNPA	(10xxx)+1+555-1212	IC
FNPA	(10xxx)+1+NPA+555-1212	IC

* When LATA boundaries cross NPA boundaries (rare).
FNPA Foreign Numbering Plan Area (area code).
HNPA Home Numbering Plan Area (area code).

At first glance, the above table appears somewhat complex. But, if you understand the concept of LATAs and carriers, it is easily understood. Essentially, all local Bell Operating Companies will maintain their own directory assistance services. When a customer dials 411 or 555-1212, he will reach a BOC directory assistant. Additionally, each long distance carrier that wishes to provide directory assistance to its customers will also have DA facilities. And, when a customer dials a directory assistant (NPA+555-1212) on a carrier, he will reach an operator of that particular long distance carrier. The key here is LATAs. If a customer wants to find a number that is within his LATA, no long distance carrier is involved. It is handled strictly by the Local Bell Operating Company. If a customer is seeking a number that is not within his LATA, he must use the services of an inter-LATA (long-distance) carrier.

TSPS Operator Services

Traffic Service Position System (TSPS) operator services will be handled much in the same fashion as directory assistance services, with a few differences. As with DAs, each Bell Operating Company and each inter-LATA carrier will maintain its own TSPS operator facilities (or cordboard I suppose, if they cannot afford TSPS). When a customer dials simply 0 (operator), he will reach a BOC TSPS operator. The BOC TSPS will be able to handle all types of intra-LATA operator-assisted traffic including (but not limited to): collect, third party billing, Bell credit card, coin, verification and emergency interrupt, and requests for emergency aid. BOC TSPS will be unable to complete calls for customers outside of the customer's LATA.

Thus, inter-LATA operator assistance will be handled by an inter-LATA carrier TSPS (IC TSPS). An IC TSPS will handle all previously mentioned types of calls that require inter-LATA transport (i.e., the call originates and terminates in different LATAs). When a customer dials 0+NXX-XXXXX or 0+NPA+NXX-XXXX, the central office will determine if the call is destined for another LATA. If it is not, the call will be sent to the Bell TSPS for appropriate handling. If the call is bound for another LATA (and his determination is made based on the NXX or NPA+NXX), then the call will be sent off to the customer's primary long-distance carrier (since only 0+ was dialed). If the customer wishes to use a different carrier's operator services, he would dial 10xxx+0+number, and the carrier specified by the 10xxx carrier access code would receive the call.

Note If a customer dials 10xxx+0+number, and the call is an intra-LATA call, he will get a recording, "We're sorry, the number you dialed cannot be reached with the carrier access code you dialed. Please check the code and try again or call your carrier for assistance." (Western Electric KS-22550 central office tape list no. 46.) Until the Bell Operating Companies can install their own TSPS facilities and networks, they will (continue to) lease capacity from AT&T TSPS. That is, AT&T will handle the intra-LATA traffic for the BOCs on a contract basis. In the meantime, AT&T will continue to handle its own long-distance operator services while the other inter-LATA carriers will have to implement their own operator networks from scratch. My estimation is that you won't be able to dial 10222+0 for an MCI TSPS operator until sometime around the year 2590. And even then they will probably be cordboard.

In addition to the changes in TSPS described above, there will be certain modifications to the software and hardware involved in the TSPS operator system. Most critical, and of paramount importance to the telecommunications enthusiast is changes in circuit associated signalling (CAS). This is signalling to and from the TSPS facility. When a customer dials 0 (operator) or 10xxx+0 (IC operator), a succession of events occurs. First, the end office seizes a trunk to the appropriate operator facility (this assumes that no access tandem is involved). The operator service facility responds with a wink (proceed signal) and the end office outpulses the CALLED number (or KP+ST if 0 only dialed). The operator service (OS) facility will then come off-hook to signal that it is ready to receive ANI information. The end office outpulses the ANI information in the format of KP+II+7 digits+ST (or ST'). If there is ANI failure, a KP+02+ST (or ST') will be sent. "ST'" stands for STart "prime", and is indicative of a coin call (i.e., dial 0 from a coin station). A normal ST terminating the ANI sequence means that the call is originating from a noncoin station. See table for ultimate description.

Inter-LATA calls MF-Pulsed

type of call	customer dials ANI	cld num
noncoin:		

direct dialed	10xxx+1+7/10d	KP+7/10d+ST''	KP+II+7d+ST
operator assist	10xxx+0	KP+ST'''	KP+II+7d+ST
special toll	10xxx+0+7/10d	KP+7/10d+ST'''	KP+II+7d+ST

coin:

direct dialed	10xxx+1+7/10d	KP+7/10d+ST	KP+II+7d+ST
operator assist	10xxx+0	KP+ST'	KP+II+7d+ST
special toll	10xxx+0+7/10d	KP+7/10d+ST'	KP+II+7d+ST

Intra-LATA calls

noncoin:

direct dialed	10xxx+1+7/10d	KP+7/10d+ST''	KP+II+7d+ST'
operator assist	10xxx+0	KP+ST'''	KP+II+7d+ST'
special toll	10xxx+0+7/10d	KP+7/10d+ST'''	KP+II+7d+ST'

coin:

direct dialed	10xxx+1+7/10d	KP+7/10d+ST	KP+II+7d+ST'
operator assist	10xxx+0	KP+ST'	KP+II+7d+ST'
special toll	10xxx+0+7/10d	KP+7/10d+ST'	KP+II+7d+ST'

Note	ST	Start
	ST'	STart prime
	ST''	Start double prime
	ST'''	STart triple prime.

Once again, the above table appears somewhat intimidating in its complexity. All these STs, ST primes, etc. Actually, the only purpose of the starts is to distinguish to the TSPS machine exactly what type of call the customer is placing and from what type of telefone he is calling. "Special toll" calls are collect, credit card, and third-party billing type calls. Here is an example of a complete dialing and outpulsing sequence for an operator service call:

from a coin fone, a customer dials 0+ (or 10xxx+) 303+979-9997. The central office would seize a trunk to the operator service facility and outpulse: KP+303+979-9997+ST'. This indicates to the operator service facility that the call is a special toll call originating from a coin telephone. The OS facility comes off-hook and the central office would then outpulse KP+00+232+9969+ST. This is he ANI information, and the ST indicates that the call is inter-LATA (if it were intra-LATA, the sequence would be terminated with ST' instead).

Perhaps now I should explain screening. Certain telefones are "screened" against placing certain types of calls. A screening code is a two digit information carrier. For instance, 00 is "identified line" (no special treatment), 01 is multiparty ONI (operator number identification), 02 is ANI failure, 06 is hotel/motel, 07 is coinless (hospital/inmate fone), 08 is inter-LATA restricted, 68 is hotel inter-LATA restricted, 78 is coinless (hospital inmate) inter-LATA restricted, etc. A 98 is an AT&T Charge-A-Call fone (those blue fuckers). More screening codes are allocated as they are needed. Note that the original TSPS screening design only allowed for single digit information digits. They were later found to be insufficient.

I believe that the operator services have been adequately covered, so I will now move on to other aspects of Equal Access.

Routing Codes

The TTC (terminating toll centre) and special routing codes will continue to be used in inter-LATA networks. These 0xx and 1xx type codes, which sometimes precede operator routing codes, will be assigned to various ICs on an individual basis. When 0xx and 1xx codes serve as pseudo-central office code, they will be coordinated such that it will avoid IC conflicts. The Numbering/Dialing Planning Group of the Central Services Organization (sounds like some sort of Communist governing body) will provide assistance where the assignment of coordinated codes is necessary.

Special Area Codes

Special area codes, also called Service Area Codes (SACs) presented the designers of Equal Access with an interesting problem. SACs are N00 type area codes, such as 700, 800, and 900. They are used for special services and unlike normal area codes, are not associated with a particular state or region. Each long distance carrier will be allocated its own exchanges in each service area code. Thus, when a customer places a call to a number in a service area code, the central office will examine the exchange of the telefone number and route the call over the proper carrier's facilities. The customer will be totally oblivious to this process. Current SACs include 700 (teleconferencing), 800 (toll free services), and 900 (dial-it services). There are currently plans under way to implement the 600 area code, although its exact uses are not yet clear.

Signalling to IC

Each long distance carrier that wishes to serve a particular LATA must establish a point of presence (POP) in that LATA. A carrier's POP is a toll office that receives toll traffic destined for another LATA. A POP is a centre for inter-LATA transport of toll traffic. This traffic will be directed to it from a Bell central office, either an end office or an access tandem (AT). An access tandem is simply a Bell office which directs long distance traffic from a number of local end offices to a number of different inter-LATA carriers. To pass call details (such as called and calling numbers) from the Bell local office to the inter-LATA carrier, a signalling system was designed that employs current multifrequency (MF) signalling protocol. When a customer dials 10xxx+(1/0)+(NPA)+NXX+, the end office will seize a trunk to the appropriate IC as determined by the 10xxx CAC (or primary carrier if no CAC is dialed).

Note This happens as soon as the customer finishes dialing the exchange, even though he may still be dialing the last four digits of he telefone number. After the end office has seized a trunk to the IC, the IC will return a wink, which is the signal to proceed. Then, the end office will send ANI information, in the format of: KP+II+10 digit ANI+ST. If the carrier is not to receive ANI information from the Bell Operating Company (i.e., they are not paying for it), then only KP+ST is sent. Presumably, by now the customer has completed dialing the last four digits of the destination telefone number, so the end office will send: KP+7 or 10 digit CALLED number+ST.

Note several things here:

1. The IC does not send a wink when it is ready to receive CALLED number information.

2. ANI information is ten digits, plus a two-digit screening code, and

3. The central office's outpulsing to the IC overlaps the customer's dialing.

Some ANI screening codes include: 00 (identified POTS), 01 (ONI multiparty), 02 (ANI failure), 06 (hotel without room identification), 07 (coinless, hospital, inmate, etc.), 08 (inter-LATA restriction), 10 (test call), 20 (AIOD calls, listed DN sent), 27 (coin call), and 95 (test call). These are the same or similar as the screening codes used in operator service signalling.

In addition to the domestic signalling design outlined above, a new international signalling system has been designed for use with Equal Access. It also uses two-stage, overlapping outpulsing. After a customer has completed dialing (10xxx)+011+CC (CC is country code), the Bell end office will seize a trunk to he appropriate IC (or international carrier, if direct routing is available). The IC/INC will respond with a wink, and the end office will outpulse: KP+1NX+YXX+CCC+ST. Each of these three groups of routing information indicate something different abut the international call being placed. The 1NX is the "international system routing code, one for each type of call routing." I have absolutely no idea what that means, and no one I have talked to at Bell, AT&T, MCI, CCITT, ITT, the CSO and FCC have any idea either. Next, the YXX is the carrier routing code. It is actually XXX, Which is the three digits of the 10xxx CAC for the particular carrier being accessed. Finally, CCC is the country code, padded with a zero if necessary.

One may wonder why the CAC is signalled forward when a trunk is seized directly to the carrier itself. The reason for this is that in some cases a direct trunk to the carrier is not available and the call must be routed through an access tandem, which is responsible for routing calls to a variety of different long distance carriers.

Switch Compatibility

Full-feature Equal Access will become available first for Western Electric #1ESS switching systems. It will be available first in generic 1E8 (1AE8 for #1A ESS). Later, generic 5E2 for #5ESS, generic 2B4 for #2B ESS, generic BCS-16 for Northern Telecom DMS-100, and generics 209 and 302 for DMS-10 will provide full-feature Equal Access capabilities in those types of end office switching equipment. The Western Electric #4ESS, #1 and 1A ESS, #5ESS, and the Northern Telecom DMS-200 machines which serve as toll offices or access tandems will be capable of receiving the new Equal Access signalling format, after required generic development. Other switches (such as all crossbar offices) will not be able to handle the new signalling format.

LATAs

LATAs, Local Access and Transport Areas, are the entire key to the administration of Equal Access. They can be thought of as miniature area codes. A telefone call can never cross a LATA boundary except on an inter-LATA carrier. However, there are certain exceptions to this. For example, in the state of Colorado, which consists of two LATAs, the local Bell Operating Company (Mountain Bell), which serves as the intra-LATA (i.e., calls to/from the same LATA) carrier, may also serve as inter-LATA (to/from different LATAs) carrier within Colorado.

There are also exceptions in the corridor region of the New York/New Jersey/Pennsylvania area.

The forty-eight continental United States consist of 161 LATAs. Some states, such as Deleware, consist of only one LATA, while others, such as Illinois, can have up to 14 or more. Each LATA is given a name. For instance, Pennsylvania consists of six LATAs: Philadelphia, Capital, Northeast, Altoona, Pittsburgh, and Erie (independent telco).

A Few Thoughts

In 1973, Chrysler, A&P, RCA, Phillips Petroleum, S.S. Kresge, Boeing Aircraft, International Harvester, Woolworth's, Greyhound, Firestone, Litton, and General Foods, among others, each reported annual profits of less than $150 million. In that same year, the Telephone Company wrote off, as being uncollectable, debts of $150 million.

In 1974, the Bell System had direct interests in at least 276 organizations, many of them not related to the telefone industry. Bell also had interlocking financial arrangements with such corporations as the Chase Manhattan Bank, IBM, Prudential Insurance, Sears Roebuck, General Motors, U.S.

Steel, and Lever Brothers. Should the need have arisen, the Bell System in 1974 could have exercised control of 400 billion dollars, fully one-third of that year's gross national product.

From Hyde, J. Edward, The Phone Book. Henry Regnery Publishing
Company, Chicago Illinois, 1976. ISBN 0-8092-8008-6.

<<> G-File: The Official Phreakers Manual: PHREAK*.DOC 214
G_PHREAK.WPS 11/20/90 11:29 AM

There are many viewpoints as to the future course of the telefone industry. The general consensus among most Telco employees is that the children of AT&T (i.e., the seven regional holding companies into which the Bell System was divided) will someday be reassembled into the original Bell System, and all will be well and good in the world of telecommunications again. I tend to disagree with this. I think that within three decades the entire telefone industry will be consolidated and nationalized. It will be owned and operated entirely by the United States Federal Government. This will accomplish several goals of the government. First, the immense revenue from telefone services will provide great financial resources for the federal government. Rates for telefone services will skyrocket far out of the range of affordability, quality of service will deteriorate to a point of unusability, and meanwhile politicians will get rich.

Second, once the government controls the telefone system, monitoring the general public will become infinitely easier. Big Brother will be able to keep and eye, or rather, an ear on the general population, and giant step forward in ultimate government control of peoples' lives will be achieved. Most people won't know anything about this, and even if they do, they won't give a shit because by then the fucking government will have already invaded every remaining private aspect of the individual's life.

To those who find it utterly unthinkable that the federal government would ever assume control of the telefone industry, I would call attention to the situation that existed between 1917 and 1919. During this time the government controlled the phone system of the United States. J. Edward Hyde sums it up beautifully:

> Between 1917 and 1919, the Federal Government did control the phone industry. Since then, the most charitable historians have blamed the subsequent mess on the First World War. Others blame it on the democrats. But the fact is that it was a fiasco of the bureaucracy's own making, combined with intracompany sabotage.

> Today, in those countries where the phone service is nationally owned, the service runs from poor to nonexistent. Would you want the government that gave you the Russian wheat deals, Defense Department overruns, Amtrak, and the Postal Service handling your phone problems?

From Hyde, J. Edward, The Phone Book. Henry Regnery Publishing Company, Chicago, Illinois, 1976. ISBN 0-8092-8008-6, p. 170.

Technical References

- Notes on the BOC intra-LATA Networks. American Telephone & Telegraph Company, 1983.
- The Phone Book. J. Edward Hyde, 1976.
- Bell System Technical Journal. Volume 58, Number 5.
- Engineering and Operations in the Bell System. American Telephone & Telegraph Company, 1983.

Acknowledgements

Karl Marx, Telenet Bob, and the scores of Telco employees in Denver, White Plains, Omaha, and North Jersey who were very helpful in patiently answering my many questions about Equal Access.

Thanks to Mack the Knife for magnetic transfer of this illustrious file, a tedious task for which I have no time.

Thanks to the following printers for their cooperation and professional manner in helping me with final production of this file:

Kinko's Print Shop
7155 West Colfax
Lakewood, CO

Office Products and Printing
5035 S. Kipling Suite B4
Littleton, CO

This has been a Mark Tabas Encounter Series production. Questions, comments, and requests may be addressed to:

Tabas
P.O. Box 620401
Littleton, CO 80162

Requests for copies of this or any other Encounter Series file are honored for free, but please enclose a self-addressed medium sized first class mailing envelope with 73 cents postage.

Special thanks to Steve Reger, who was kind enough to shoot my neighbor's dog, whose incessant barking constantly distracted me as I labored to complete this file.

(for Amy) cl/KIABB!/jd

Equal Access and Modem Autodialers by Shadow 2600

Now that AT&T is being divested of its local telephone companies, phone customers across the nation have to choose their long distance carrier as equal access is phased in. Advertising campaigns emphasize such aspects as low rates and operator assistance, but no one mentions a factor that will affect modem users who use auto dialers for long distance calls. Not all of the alternate long distance carriers provide called party answering supervision on all calls. Called party answering supervision basically has the telephone company start billing only when the called party answers the telephone. However, many of the alternate long distance companies still operate with the "fixed timeout" basis for charging. That is, if a call is held for a fixed length of time (usually 30 seconds) the charging starts, whether or not the call was answered. This could cause modem owners large bills if they use autodialers to make long distance calls. Modems are usually set up to wait up to one minute when attempting to make a call, and thus have to timeout through busy signals, long call setup sequences, extender waits, and similar problems. This could result in many billed but never answered calls.

Some of the other carriers provide it on calls to some cities, and others not support it at all. Only AT&T Communications provides called party answering supervision on all calls to all points at this time. It is almost impossible to get information on how a long distance company charges its calls as as they don't want to reveal how their billing is handled. The alternate carriers get called party supervision when the destination location goes equal access. However, there has been no quick action on the part of the alternate long distance companies to make use of the supervision data as they would have to get equipment for passing the information back to the billing computer at the originating point. Thus called party answering supervision information often ends up being ignored by these carriers even when available.

Another point to remember is that called party answering supervision's availability depends on whether the destination has equal access, not the originating location. The lower long distance rates of alternate long distance rates must be weighed against the time out problem as it affects autodialing modems. One way to circumvent this is merely to set your modem to a shorter waiting-for-connect time, but this may not provide enough time for the call to go through.

For more information on this and other telecommunications topics call the Private Sector BBS at (201) 366- 4431]

Toward Universal Information Services Via ISDN

Phrack Inc.

Volume One, Issue Two, Phile #6 of 9
by Taran King

From PROTO newsletter of AT&T Bell Laboratories

Phase One
The Present

The local network of today, although still largely voice-oriented, is already on the path to Universal Information Services. Lightguide fiber is dramatically expanding the capacity of local networks, helping to lower the costs and increase the demand for high-band width, Information Age services. And public networks are increasingly digital and geared for data and special services. For example:

- The AT&T Network Systems 5ESS (TM <riiiight>) switch, designed by Bell Laboratories, can serve as the hub of a local deployment of remote modules at locations up to 100 miles from a host central office.

- The Integrated Special Services Network (ISSN) is a channel network that provides special services, customer control options and digital private lines rearrangeable under software control. The ISSN incorporates digital carrier terminating equipment such as the D4 Channel Bank, D5 Digital Terminal System and Digital Access and Cross-connect System (DACS).

- The New Centrex is bringing greater levels of customer control, improved services and a broad range of data capabilities to the business customer.

Today's public networks consist of multiple or overlay networks. The public switched network, or circuit network, mainly for voice, is the base network. Two kinds of overlay networks provide special services. Channel networks carry private lines leased by large customers and transmit much of today's data and image traffic; they also handle traffic for network operations support. Packet networks carry data communications, while packet switching is used internally to public networks for common channel signaling to set up, route and take down calls, or to give customers information. "Overlay networks help telecommunications companies efficiently meet growing demand for digital transmission and special services," says Stan Johnston, Market Planning Manager, Network Systems Evolution, in AT&T Network Systems. "Their integration into a single network, however, would be still more effective."

Phase Two
The Integrated Services Digital Network (ISDN)

The ISDN is a concept to which AT&T is committed - and it's the foundation for Universal Information Services. The central idea of ISDN, as AT&T Network Systems sees it, is to provide an individual user a link to the local central office of generous band-width - a digital subscriber line that can carry 144,000 bits per second (sure beats 2400 baud!). The bandwidth is subdivided into two 64,000-bit channels, which may carry voice or data or both, and one 16,000-bit channel for packetized signaling information or data transport. Such a link provides convenient "integrated" network access by accommodating voice, data and signaling over a single line.

The ISDN will make it easier for a customer to get varied services from public and private networks. More bandwidth for big customers will be available through another ISDN access standard, the extended digital subscriber line, which provides 1.5 billion bits per second as 24 channels of 64,000 bits each.

In 1986, new software from Bell Labs will enable the 5ESS switch to accommodate ISDN-sized 144,000-bit channels that standardize and simplify subscribers' use of local networks. AT&T is committed to future products that will also be ISDN-compatible. Other vendors, too, some of whom already plan to build premises, terminal, and other equipment to ISDN standards, will make ISDN a cooperative effort.

By providing integrated digital access to networks, ISDN will make important progress toward the goal of Universal Information Services. But overlay networks will continue to divvy up the transport job. And messages needing less than 144,000 bits per second will not fill their allotted bandwidth, leaving capacity under utilized.

Phase Three
Universal Information Services

Rooted in the fertile ground of 5ESS switches, ISDN equipment and technologies such as wideband packet transport, Universal Information Services will bear fruit during the 1990s. From a single kind of network will hang services as different as apples, oranges and pears. Just as network access was integrated in ISDN, transport functions will increasingly be integrated by powerful new network equipment evolved from equipment developed for the ISDN. Where customers once got standard-sized ISDN channels, they'll get big bandwidth for large jobs, little bandwidth for small jobs.

Toward Universal Information Services via ISDN

Phase one, the present. The local network of today, although still largely voice oriented, is already on the path to Universal Information Services. Lightguide fiber is dramatically expanding the capacity of local networks, helping to lower the costs and increase the demand for high-bandwidth, Information Age services. And public networks are increasingly digital and geared for data and special services. For example:

- The AT&T Network Systems 5ESS switch, designed by Bell Laboratories, can serve as the hub of a local digital network through deployment of remote modules at locations up to 100 miles from a host central office.
- The Integrated Special Services Network (ISSN) is a channel networks that provides special services, customer control options and digital private lines rearrangeable under software control. The ISSN incorporates digital carrier terminating equipment such as the D4 Channel Bank, D5 Digital Terminal System and Digital Access and Cross-connect Systems (DACS).
- The New Centrex is bringing greater levels of customer control, improved services and a broad range of data capabilities to the business customer.

Todays public networks consist of multiple or overlay networks. The public switched network, or circuit network, is the base network. Two kinds of overlay networks provide special services. Channel networks carry private lines leased by large customers and transmit much of today's data and image traffic; they also handle traffic for network operations support. Packet networks carry data communications, while packet switching is used internal to public networks for common channel signaling to set up, route and take down calls, or to give customers information.

"Overlay networks help telecommunications companies efficiently meet growing demand for digital transmission and special services," says Stan Johnston, Market Planning Manager, Network Systems Evolution, in AT&T Network Systems. "Their integration into a signal network, however, would be still more effective."

Phase two, the Integrated Services Digital Network (ISDN). The ISDN is a concept to which AT&T is commited--and it's the foundation for Universal Information Services. The central idea of ISDN, as AT&T Network Systems sees it, is to provide an individual user a link to the local central office of generous bandwidth--a digital subscriber line that can carry 144,000 bits per second. The bandwidth is subdivided into two 64,000-bit channels, which may carry voice or data or both, and one 16,000-bit channel for packetized signaling information or data transport. Such a link provides convenient "integrated" network access by accommodating voice, data and signaling over a single line.

The ISDN will make it easier for a customer to get varied services from public and private networks. More bandwidth for big customers will be available through another ISDN access standard, the extended digital subscriber line, which provides 1.5 million bit per second as 24 channels of 64,000 bits each.

In 1986, new software from Bell Labs will enable the 5ESS switch to accommodate ISDN-sized 144,000-bit channels that standardize and simplify subscribers' use of local networks. AT&T is committed to future products that will also be ISDN-compatible. Other vendors, too, some of whom already plan to build premises, terminal and other equipment to ISDN standards, will make ISDN a cooperative effort.

By providing integrated digital access to networks, ISDN will make important progress toward the goal of Universal Information Services. But overlay networks will continue to divvy up the transport job. And messages needing less than 144,000 bits per second will not fill their allotted bandwidth, leaving capacity underutilized.

Phase three, Universal Information Services. Rooted in the fertile ground of 5ESS switches, ISDN equipment and technologies such as wideband packet transport, Universal Information Services will bear fruit during the 1990s. From a single kind of network will hang services as different as apples, oranges and pears. Just as network access was integrated in ISDN, transport functions will increasingly be integrated by powerful new equipment evolved from equipment developed for the ISDN. Where customers once got standard-sized ISDN channels, they'll get big bandwidth for large jobs, little bandwidth for small jobs.

*** retyped from PROTO, AT&T Bell Laboratories report to executives on new technologies, without written permission from the editors. (heh, heh.)

Subscriptions: $15.00 per year, published bi-monthly. Send check payable to "Bell Laboratories PROTO," to PROTO Circulation Manager, Room 3E-230, 150 John F. Kennedy Parkway, Short Hills, N.J. 07078.

:LIQUID:CRYSTAL:
wisdom is safety

MCI Overview

Metal Shop
Headquarters of Phrack Newsletter
(314) 432-0756

Written on 11/16/85 by Knight Lightning & Taran King

MCI Communications Corporation, headquartered in Washington, D.C., provides a full range of domestic and international telecommunications services, including voice and data, telex and cable, paging and mobile telephone, and time sensitive message delivery.

Since its founding in 1968, MCI has grown to more than $1.6 billion in annual sales and serves more than 1.9 million business, residential and government customers through its four major business units:

- MCI Telecommunications
- MCI Airsignal

- o MCI International
- o MCI Digital Information Services

MCI Telecommunications

MCI Telecommunications provides domestic interstate long distance service throughout all 50 states, plus Puerto Rico, the U.S. Virgin Islands, and major calling areas of Canada. It is also authorized to provide varying degrees of intrastate long distance service in some states.

MCI also is the first long distance carrier other than AT&T to offer direct dial service overseas. International telephone service is available to all residential and commercial customers (with the exception of Private Line customers). In October, 1984 the first international service agreements were announced with the following countries: Argentina, Belgium, Brazil, East Germany, Greece, United Arab Emirates, and the United Kingdom.

Total capital investment in MCI's long distance network is approximately $2 billion. MCI's network, the second largest in the U.S., employs microwave optical fiber, satellite and various digital transmission technologies.

Subscribers	Domestic Long Distance (as of 10/84)
Residential	1.4 million
Commercial	.3 million
Total	1.7 million

Operations	(as of 10/84)
Network Miles	20,543 (microwave, optical fiber, satellite)
Circuits	238,000
Employees	9,500 (full-time, approx.)

MCI Airsignal

MCI Airsignal provides personal message delivery and car telephone services. MCI Message Service is offered in more than 50 metropolitan areas. In 1984, service will commence in New York City, Baltimore-Washington, Los Angeles, and Chicago. MCI car telephone service is offered in 20 markets.

Personal Message Delivery Services:

Alphanumeric Message Service
Displays up to 40-character message using letters and/or numbers. Memory and recall ability. Alerts subscriber with a silent visual alert or a soft tone.

Display Message Service
Displays up to 24-digit message (e.g., phone number, stock quotes, sales figures, coded messages). Memory and recall capability. Alerts customer to message with a silent visual alert or a soft tone.

Tone Message Service
Notifies customer of a message with a soft tone.

Voice Message Service
Receives message in actual voice of caller.

Express Message Service
Receives and stores messages. Instantly alerts subscriber via pager when a message is received.

Car Telephone Service
Enables customers to place calls to or receive calls from anywhere in the world, 24 hours a day, as they travel in their cars. With the advent of new cellular technology,

both the quality and the accessibility of car telephone service will vastly improve.

MCI has thus far obtained franchises to operate a new kind of mobile phone service, cellular telephone, in Minneapolis and Pittsburgh, and has received favorable decisions from FCC administration law judges authorizing service in Los Angeles, Denver-Boulder, and Kansas City. MCI has applied for licenses to provide cellular service in 81 metropolitan areas.

MCI Airsignal Branch Sales Offices

Personal Message Service/Conventional Mobile Phone Service

Birmingham	(205)	942-2924
Sacramento	(916)	444-2350
Memphis	(901)	682-9658
Cleveland	(216)	464-7311
Dallas	(214)	788-5111
Fresno	(209)	486-7410
Las Vegas	(702)	382-7461
Denver	(303)	778-7878
Portland	(503)	227-2556
Philadelphia	(215)	677-9845
Atlanta	(404)	252-2114
West Florida	(813)	875-3404
Minneapolis	(612)	544-8175
Kansas City	(913)	648-8090
Miami	(305)	491-0122
Pittsburgh	(412)	343-1611
Houston	(713)	464-2516
Bakersfield	(805)	832-2346

Cellular Telephone Offices

Minneapolis-St. Paul	(612)	544-3312
Los Angeles	(714)	527-0385
Elsewhere in California	(800)	344-3455
Headquarters - Washington, D.C.	(202)	429-9660

MCI International

MCI International provides private-line voice service to several overseas countries, and data and message services, including telex, cablegram, leased channel, and packet switching communications, to more than 200 overseas points. MCI has moved into two new areas of service: International direct-dial telephone service and international electronic mail and hard-copy delivery services.

... International Record Services

Telex Service

(domestic and international) Permits instantaneous, two-way, written communications with other subscribers worldwide. Customers can send messages at any time, even though the receiving terminal may be unattended. MCI International offers access to its telex service from a variety of terminals and networks; not only subscribers with telex terminals but also those with communicating word processors, data terminals or computers that communicate over telephone lines can take advantage of MCI International telex service. To subscribers connected to its own telex network, MCI International offers World Message Services--a package of communications offerings including telex, cablegram and MCI Mail services. Various service enhancements are available to save time, improve operating efficiency and simplify records keeping for telex users.

Cablegram Service

The traditional means of international written communications, offers flexibility in delivery and economical rates for shorter messages. Cablegrams can be delivered to virtually any overseas point.Subscribers with telex terminals or various other types of equipment can access and TELUS cablegram switch and take advantage of such service enhancements as abbreviated addressing and departmental billing.

Leased Channel Service

Provides an exclusive line between a U.S. firm and it's overseas office for private communications 24 hours a day. Each MCI International leased channel is tailored to meet the needs of a specific customer for teleprinter, facsimile, voice and/or data traffic. For subscribers with several offices requiring private communications with each other, MCI International offers a versatile message-switching service. Voice/data leases can be configured to meet a whole array of communicating needs; for example, one channel might carry data traffic from a computer at night, voice communications during office hours, and simultaneous teleprinter messages at any time. Data channels can handle requirements for traffic at any speed from 1200 bits per second to 1.544 megabits per second.

IMPACS Service

Uses packet-switching technology to provide international communications service between data terminals and computers. Impacs offers on-line, real-time connections and enables many types of incompatible systems to communicate. Impacs service offers virtually error-free transmission because of the error-detection and retransmission capability of the network.

Instalink Service

Allows businesses overseas to use regular telex equipment to access remote computing systems and databases in the U.S. Subscribers can retrieve data from a computer-based information service or use a computing system connecting to a packet-switching network in the U.S.

International Facsimile Service
Enables subscribers to send duplicates of original documents overseas quickly and efficiently, even when neither the sender or the receiver has facsimile transmission equipment, or when the sender and receiver have incompatible equipment.

DATEL Service
Provides automatic or voice-coordinated data transmission at speeds up to 2400 bits per second. Either digital or analog facsimile traffic can be transmitted via Datel. Datel facilities are conditioned to ensure high-quality transmission. The MCI International switching center allows communications between incompatible terminals.

Maritime Services
Provide instant, high--quality contact between ships at sea or offshore rigs, and between these vessels and land-based subscribers worldwide.

... International Voice Services

Private Line Service
Provides, fast, easy access to a single overseas location at an economical monthly rate. This technically efficient system maximizes the use of line capacity by recognizing idle time and assigning a speaker to a transmission path only when the path is needed. Users can dial a four-digit

extension from a regular business phone to reach a key overseas location.

International Mail Services

World Message Service
Subscribers can access the domestic electronic mail and hard-copy delivery offerings of MCI Mail. In addition, MCI International is developing fast, low-cost services that will deliver electronic messages and high-quality printed documents worldwide.

... Customer Service

The Customer Trouble Reporting Assistance Center
At MCI International Addresses
Customer concerns such as equipment maintenance and service performance questions. Customer service specialists, on duty 24 hours a day on business days, answer questions and electronically route service requests to technicians nationwide.

MCI Digital Information Services Corp.
MCI Digital Information Services, MCI's newest unit, provides high-speed, low-cost, time-sensitive message delivery (MCI Mail), either electronically or via hard copy.

MCI Mail
Provides time-sensitive document delivery to anyone, anywhere vial MCI's long-distance telephone network. MCI Mail can reach a recipient instantly, in four hours or less, or overnight by noon the next day. Prices are as much as 90 percent lower than comparable time-sensitive mail delivery services. MCI Mail can be delivered electronically, terminal to terminal, or laser printed on letterhead stationery with the customer's signature.

MCI Mail customers can even order gifts and services direct through MCI Mail, ranging from software and paper for personal computers to investment advisory services to travel specials.

There are no sign-up, monthly service charges or "connect time" charges for MCI Mail. MCI Mail can be used by virtually any personal computer, word processor, electronic typewriter, data terminal, telex, or other digital communications device. The service is accessed by a local telephone call or 800 number.

... MCI Mail

Instant
Delivery to an "electronic" mailbox.

Four-Hour
Paper delivery by courier to 17 major metropolitan areas regardless of point of origin.

Overnight
paper delivery by courier by noon the next day in 20,000 continental U.S. cities.

MCI Letter
Transmitted electronically to the MCI digital postal center nearest its destination, then delivered locally by the U.S. Postal Service.

Telex Dispatch
Enables MCI Mail subscribers to transmit messages to the more than 1.6 million telex subscribers worldwide.

Volume Mail
Enables customers to send large mailings in a variety of letter formats, at substantial savings in delivery time and expense.

Look for more MCI Files coming to Metal Shop soon!
This has been a Knight Lightning Presentation

Reference Tables

Just some notes that you will always try to find but can never!

Using MCI Calling Cards

By Knight Lightning of the 2600 Club!

Volume One, Issue One, Phile #5 of 8
Phrack Inc.

How to dial international calls on MCI

"Its easy to use MCI for international calling."

1. Dial your MCI access number and authorization code (code = 14 digit number, however the first 10 digits are the card holders NPA+PRE+SUFF).
2. Dial 011
3. Dial the country code
4. Dial the city code and the PRE+SUFF that you want.

Countries served by MCI

Country	code	Country	code
Algeria	213	New Zealand	064
Argentina	054	Northern Ireland	044
Australia	061	Oman	968
Belgium	032	Papua New Guinea	675
Brazil	055	Qatar	974
Canada	Use Area Codes	Saudi Arabia	966
Cyprus	357	Scotland	044
Denmark	045	Senegal	221
Egypt	020	South Africa	027
England	044	Sri Lanka	094
German Democratic Rep.	037	Sweden	046
Greece	030	Taiwan	886
Jordan	962	Tanzania	255
Kenya	254	Tunisa	216
Kuwait	965	United Arab Emirates	971
Malawi	265	Wales	044

Thats 33 countries in all. To get the extender for these calls dial 950-1022 or 1-800-624-1022.

For local calling

1. Dial 950-10222 or 1-800-624-1022
2. Wait for tone
3. Dial "0", the area code, the phone number, and the 14 digit authorization code. You will hear 2 more tones that let you know you are connected.

Knight Lightning
The 2600 Club!

AT&T International Dialing Country Codes as of 85/2/17

File by: Lock Lifter

United Kingdom/Ireland

Ireland	353
United Kingdom	44

Europe

Andorra	33
Austria	43
Belgium	32
Cyprus	357
Czecholslovakia	42
Denmark	45
Finland	358
France	33
German Democratic Republic	37
Germany, Federal Republic of	49
Gibraltar	350
Greece	30
Hungary	36
Iceland	354
Italy	39
Liechtenstein	41
Luxembourg	352
Monaco	33
Netherlands	31
Norway	47
Poland	48
Portugal	351
Romania	40
San Marino	39
Spain	34

Sweden	46
Switzerland	41
Turkey	90
Vatican City	39
Yugoslavia	38

Central America

Belize	501
Costa Rica	506
El Salvador	503
Guatemala	502
Honduras	504
Nicaragua	505
Panama	507

Africa

Algeria	213
Cameroon	237
Egypt	20
Ethiopia	251
Gabon	241
Ivory Coast	225
Kenya	254
Lesotho	266
Liberia	231
Libya	218
Malawi	265
Morocco	212
Namibia	264
Nigeria	234
Senegal	221
South Africa	27
Swaziland	268
Tanzania	255
Tunisia	216
Uganda	256
Zambia	260
Zimbabwe	263

Pacific

American Samoa	684
Austrailia	61
Brunei	673
Fiji	679
French Polynesia	689
Guam	671
Hong Kong	852
Indonesia	62
Japan	81
Korea, Republic of	82
Malaysia	60
New Caledonia	687
New Zealand	64
Papua New Guinea	675
Philippines	63
Saipan	670
Singapore	65
Taiwan	886
Thailand	66

Indian Ocean

Pakistan	92
Sri Lanka	94

South America

Argentina	54
Bolivia	591
Brazil	55
Chile	56
Colombia	57
Ecuador	593
Guyana	592
Paraguay	595
Peru	51
Suriname	597
Uruguay	598
Venezuela	58

Near East

Bahrain	973
Iran	98
Iraq	964
Israel	972
Jordan	962
Kuwait	965
Oman	968
Qatar	974
Saudi Arabia	966
United Arab Emirates	971
Yemen Arab Republic	967

Caribbean/Atlantic

French Antilles	596
Guantanamo Bay (US Navy Base)	53
Haiti	509
Netherlands Antilles	599
St. Pierre and Miquelon	508

India

India 91

Canada

To call canada, dial 1 + area code + local number.

Mexico

To call mexico, dial 011 + 52 + city code+ local number.

Note Do not forget about the time difference when calling outside of your time zone. Calling cards can be used over seas to call back into the u.s. For further information call toll-free 1-800-874-0000. Dial '#' after the complete number to make the call go through faster.

International Dialing Codes
Country + Routing

Typed by The Dagda Mor
Edited by The Jammer

To dial international calls

International Access Code + Country code + Routing code

Example

To call Frankfurt, Germany, you would do the following:

011 + 49 + 611 + (# wanted) + # sign(octothrope)

The # sign at the end is to tell Bell that you are done entering in all the needed info. Here is the list of Country Codes, listed next to the country, and the routing codes listed next to the city.

Andorra	33	Argentina	54
all points	078	Buenos Aires	1
Australia	61	Austria	43
Melbourne	3	Innsbruck	5222
Sydney	2	Vienna	222
Bahrain	973	Belgium	32
no routing needed		Antwerp	31
		Brussels	2

Belize	501	Bolivia	591
no routing needed		La Paz	2
Brazil	591	Chile	56
Brasilia	61	Santiago	2
Rio de Janeiro	21	Valparaiso	31
Sao Paulo	11		
China	86	Colombia	56
Tainan	62	none needed	

Taipei	2		
Costa Rica	506	Cyprus	357
no routing needed		Nicosia	21
Denmark	45	Ecuador	593
Aalborg	8	Cuenca	4
Copenhagen	1 or 2	Quito	2
El Salvador	503	Fiji	679
no routing needed		none needed	
France	33	Germany	49
Bordeaux	56	Berlin	30
Marseille	91	Bonn	228
Nice	93	Frankfurt	661
Paris	1	Munich	89
German Republic	37	Greece	30
Berlin	2	Athens	1
		Rhodes	241
Guam	671	Guatamala	502
no routing needed		Guatemala City	2

Guyana	592	Haiti	509
Georgetown	02	Port Au Prince	1
Hoduras	504	Hong Kong	852
no routing needed		Hong Kong	5
		Kowloon	3

Indonesia	62	Iran	98
Jakarta	21	Teheran	21
Iraq	964	Ireland	353
Baghdad	1	Dublin	1
		Galway	91
Israel	978	Italy	39
Haifa	4	Florence	55
Jerusalem	2	Naples	81
Tel Aviv	3	Rome	6
		Venice	41
Ivory Coast	225	Japan	81
no routing needed		Hiroshima	822
		Tokyo	3
		Yokohama	45
Kenya	254	Korea	82
Nairobi	2	Pusan	51
		Seoul	2
Kuwait	965	Liberia	231
no routing needed		none needed	
Libya	218	Lechtenstein	4
Tripoli	21	All points	75

Luxembourg	352	Malaysia	60
no routing needed		Kuala Lumpur	3

Monaco	33	Netherlands	31
All points	93	Amsterdam	20
		Rotterdam	10
		The Hague	70
New Caledonia	687	New Zealand	64
no routing needed		Auckland	9
		Wellinton	4
Nicaragua	505	Nigeria	234
Managua	2	Lagos	1
Norway	47	Panama	507
Bergen	5	none needed	
Oslo	2		
Papua New Guinea	675	Paraguay	595
no routing needed		Asuncion	21
Peru	51	Phillippines	63
Arequipa	542	Manila	2
Lima	14		
Portugal	351	Romania	40
Lisbon	19	Bucuresti	0
San Marino	39	Saudi Arabia	966
All points	541	Riyadh	1

Senegal	221	South Africa	27
no routing needed		Cape Town	21
		Pretoria	12
Spain	34	Sri Lanka	94
Barcelona	3	Colombo	1
Canary Islands	28		
Madrid	1		
Seville	54		
Suriname	597	Sweden	46
no routing needed		Goteborg	31
		Stockholm	8
Switzerland	41	Tahiti	689
Berne	31	none needed	
Geneva	22		
Lucerne	41		
Zurich	1		
Thailand	66	Tunisia	216
Bangkok	2	Tunis	1
Turkey	90	United Arab Emirates	971
Istanbul	11	Abu Dhabi	2
		Ajman	6
		Al Ain	3
		Aweir	49
		Dubai	4
		Fujairah	91
		Jebel Dhana	5
		Sharjah	6
		Umm-Al-Quwain	6

United Kingdom	44	USSR	7
Belfast	232	Kiev	044
Cardiff	222	Leningrad	812
Edinburgh	31	Minsk	017
Glasgow	41	Moscow	095
Liverpool	51	Tallinn	0142
London	1		

Vatican City	39	Venezuela	58
All points	6	Caracas	2
		Maracaibo	61

Yugoslavia	38
Belgrade	11
Zagreb	41

MAX Access Ports
Lexitel Corporation

Adrian, Mi	313-263-0191	Livonia, Mi	313-261-6970
Akron, Oh	216-275-9814	Los Angeles	213-624-9041
Ann Arbor, Mi	313-451-2121	Louisvilley	502-568-6204
Atlanta, Ga	404-525-1769	Marion, Oh	614-387-1011
Avon Lake, Oh	216-933-2823	Mckeesport	412-664-4870
Baden, Pa	412-869-1360	Mentor, Oh	216-255-1645
Baltimore, Md	301-444-7280	Middletown	513-423-1066
Beaver Fallsa	412-847-3640	Milwaukee	414-933-1880
Birmingham, Mi	313-649-0730	Minneapolis	612-375-0280
Boston, Ma	617-267-9134	Monessen, Pa	412-684-8710
Buffalo, Ny	716-854-0802	Morton Grove	312-950-1066
Butler, Pa	412-285-9081	Newark, Nj	201-624-5040
Canton, Oh	216-455-1425	Newark, Oh	614-349-8754
Chicago, Il	312-950-1066	New Castle	412-656-9420
Chillicothe, Oh	614-772-1066	New York, Ny	212-950-1066
Cincinnati, Oh	513-421-1880	Oak Lawn, Il	312-950-1066
Cleveland, Oh	216-771-6614	Philadelphia	215-751-9711
Columbus, Oh	614-950-1066	Pittsburg	412-391-9532
Dallas, Tx	214-653-1047	Plymouth, Mi	313-451-2121
Dayton, Oh	513-223-0366	Pontiac, Mi	313-332-0500

Detroit, Mi	313-950-1066	Port Huron	313-982-7115

Elk Grove, Il	312-950-1066	Phoenix, Az	602-242-0252
Elyria, Oh	419-323-4431	Queens, Ny	718-204-7330
Findlay, Oh	419-424-5934	Sandusky, Oh	419-625-1289
Gleenshaw, Pa	412-486-7394	Sharon, Pa	412-983-0100
Grand Rapids	616-456-7925	Springfield	513-950-1066
Greensburg, Pa	412-836-8110	Steubenville	614-283-1756
Hackensack, Nj	201-342-2815	St. Louis	314-289-9100
Houston, Tx	713-224-0982	St. Paul, Wi	612-375-0280
Indiana, Pa	412-349-8760	Toledo, Oh	419-255-1316
Indianapolis	317-638-4442	Troy, Oh	513-335-2303
Kalamazoo, Mi	616-342-0266	Turtle Creek	412-823-1500
Kansas City, Mo	816-474-6193	Washington	202-479-4411
Kokomo, In	317-453-9932	Washington	412-225-1800
La Grange, Il	312-950-1066	Warren, Mi	313-268-9120
Lancaster, Oh	614-687-0159	Xenia, Oh	513-376-2991
Lansing, Mi	517-950-1066	Youngstown	216-746-2021
Lafayette, In	317-423-5492	Zanesville	614-454-6815

Metrofone Access Numbers

Anaheim, Ca	714-527-7055	Los Angeles	213-992-8282
Atlanta, Ga	404-223-1000	Los Angeles	213-202-6117
Austin, Tx	512-474-6057	Miami, Fl	305-326-3300
Baltimore, Md	301-659-7700	Milwaukee	414-277-1805
Beaumont, Tx	713-833-9331	Minneapolis	612-370-9000
Boston, Ma	617-482-3222	New Orleans	504-566-8500
Buffalo, Ny	716-852-9200	New York, Ny	212-732-7430
Chicago, Il	312-853-4700	Newark, Nj	201-645-9220
Cincinnati, Oh	513-241-1747	Oakland, Ca	415-836-6900
Cleveland, Oh	216-861-5163	Oklahoma Cty	405-232-9011
Columbus, Oh	614-224-0577	Omaha, Ne	402-422-1120
Culver City, Ca	213-410-0078	Philadelphia	215-351-0100
Dallas, Tx	214-742-4500	Pittsburgh	412-261-5720
Dayton, Oh	513-228-1576	Reno, Nv	702-329-1025
Denver, Co	303-623-5326	Richmond, Va	804-225-1920
Detroit, Mi	313-963-4847	St. Louis	314-342-1130
El Monte, Ca	213-350-1028	Sacramento	916-443-6921
Elk Grove, Il	312-981-8870	San Antonio	512-224-9600
Ft. Lauderdale	305-462-3530	San Diego	714-233-0327
Ft. Worth, Tx	817-338-1639	San Frncisco	415-956-0162
Hackensack, Nj	201-487-3155	San Jose, Ca	408-947-7606
Hartford, Ct	203-522-0003	San Mateo	415-579-6001

Hawthorne, Nj ...	201-427-1100	Santa Ana	714-972-9515
Hinsdale, Il	312-986-0566	Seattle, Wa ..	206-382-0910
Houston, Tx	713-224-9417	Skokie, Il ...	312-679-8120
Huntington Bch ..	714-972-8515	Syracuse, Ny .	315-474-3911
Indianapolis	317-635-6284	Toledo, Oh ...	419-243-1046
Kansas City, Ks .	913-621-3186	Washington ...	202-737-2051

Long Island, Ny .	516-443-5402
Los Angeles, Ca .	213-629-1026

Area Codes In Numerical Order

By The Jammer

201	Newark, New Jersey	519	London, Ontario
202	Washington D.C, (all)	601	Mississippi, (all)
203	Connecticut, (all)	602	Arizona, (all)
205	Alabama, (all)	603	New Hampshire, (all)
206	Seattle, Washington	605	South Dakota, (all)
207	Maine, (all)	606	Winchester, Kentucky
208	Idaho, (all)	607	Binghamton, New York
212	Bronx, Nyc, New York	608	Madison, Wisconsin
212	Manhattan, Nyc, New York	609	Trenton, New Jersey
213	Los Angeles, California	612	St. Paul, Minnesota
214	Dallas, Texas	613	Ottawa, Ontario
215	Philadelphia, Pennsylvania	614	Columbus, Ohio
216	Cleveland, Ohio	615	Nashville, Tennessee
217	Springfield, Illinois	616	Grand Rapids, Michigan
218	Duluth, Minnesota	617	Boston, Massachusetts
219	Gary, Indiana	618	Alton, Illinois
301	Maryland, (all)	619	San Diego, California
303	Colorado, (all)	700	Teleconference, (all)
304	West Virginia, (all)	701	North Dakota, (all)
305	Miami, Florida	702	Nevada, (all)
305	Orlando, Florida	703	Alexandria, Virginia
307	Wyoming, (all)	704	Charlotte, N. Carolina
308	Abott, Nebraska	705	North Bay, Ontario

309	Peoria, Illinois
312	Chicago, Illinois
313	Detroit, Michigan
314	St. Louis, Missouri
315	Syracuse, New York
316	Wichita, Kansas
317	Indinapolis, Illinois
318	Lake charles, Lousiana
319	Davenport, Iowa
401	Rhode Island, (all)
402	Omaha, Nebraska
404	Atlanta, Georgia
405	Oklahoma City, Oklahoma
712	Councilbluffs, Iowa
713	Houston, Texas
714	Anaheim, California
715	Bay City, Wisconsin
716	Buffalo, New York
716	Rochester, New York
717	Harrisburg, Pnsylvnia
800	Toll Free, (all)
801	Utah, (all)
802	Vermont, (all)
803	South Carolina, (all)
804	Richmond, Virgina
805	Bakersfield, Calif.

406	Montana, (all)
408	San Jose, California
412	Pittsburg, Pennsylvania
413	Springfield, Massachusetts
414	Milwaukee, Wisconsin
415	San Francisco, California
416	Toronto, Ontario
417	Joplin, Missouri
418	Quebec, Quebec
419	Toledo, Ohio
501	Arkansas, (all)
502	Frankfort, Kentucky
503	Oregon, (all)
504	New Orleans, Louisiana
504	Baton Rouge, Louisiana
505	New Mexico, (all)
507	Rochester, Minnesota
509	Pullman, Washington
512	Austin, Texas
513	Cincinnati, Ohio
514	Montreal, Quebec
515	Des Moines, Iowa
516	Hempstead, New York
517	Lansing, Michigan
518	Albany, New York
806	Amarillo, Texas
807	Thunder Bay, Ontario
808	Hawaii, (all)
809	Bermuda, (all)
809	Bahamas, (all)
809	Puerto Rico, (all)
809	Virgin Islands, (all)
812	Evansville, Indiana
812	Dade park, Kentucky
814	Johnston, Pennsylvania
815	Rockford, Illinois
816	Independence, Missouri
817	Fort Worth, Texas
818	Burbank, California
819	Trois Riv., Quebec
900	Dial-it, (all)
901	Memphis, Tennessee
904	Talahassee, Florida
906	Escanaba, Michigan
907	Alaska, (all)
912	Savannah, Georgia
913	Kansas City, Kansas
915	El Paso, Texas
916	Sacramento, California
918	Tulsa, Oklahoma
919	Raleigh, N. Carolina

TAC Dialups Sorted by Location 85/11/26

Volume One, Issue Two, Phile #5 of 9
Phrack Inc.

Updated from November 26, 1985
Tac Dialups taken from Arpanet by Phantom Phreaker

```
State/Country     300 Baud, 300 Type, 1200 Baud, 1200 Type
```

Alabama

Anniston Army Depot [M]

```
(ANNIS-MIL-TAC)   205-235-6285, (R4), 205-235-7650,, B/V
                  205-237-5731, (R8), 205-237-5731, (R8), B/V
                  205-237-5770, (R8), 205-237-5779, (R8), B/V
                  205-237-5805, (R8), 205-237-5805, (R8), B/V
```

Note When accessing the Anniston TAC you must first enter a <RETURN>, then enter DDN <RETURN>. After you receive CLASS DDN START, proceed as normal.

Gunter AFS [M]

```
(GUNTER-TAC)      205-279-3576
                  205-279-4682
```

Redstone Arsenal [M]

```
(MICOM-TAC)       [none known]
```

Arizona

Ft. Huachuca [M]

(HUAC-MIL-TAC)   [none known]

Yuma [M]

(YUMA-TAC)   602-328-2186,, 602-328-2186,, B/V
602-328-2187,, 602-328-2187,, B/V
602-328-2188,, 602-328-2188,, B/V

California, Northern

Alameda [M]

(ALAMEDA-MIL-TAC)   [none known]

Menlo Park [M]

(SRI-MIL-TAC)   415-327-5440, (R3), 415-327-5440, (R3), B

(USGS3-TAC) [M]   [no dialups]

Moffett Field [M]

(AMES-TAC)   [no dialups; contact NSC for access]

William Jones, 415-694-6482
, FTS-494-6482
, AV-359-6482

Monterey [M]

(NPS-TAC)   [none known]

Sacsamento [M]

(MCCLELLAN1-MIL-TAC)

[none known]

(MCCLELLAN2-MIL-TAC)

[none known]

Stanford [A]

(SU-TAC) 415-327-5220

California, Southern

China Lake [M]

(NWC-TAC) [none known]

Edwards AFB [M]

(EDWARD-MIL-TAC) [none known]

El Segundo [M]

(AFSC-SD-TAC) 213-643-9204,, 213-643-9204,, B/V

Los Angeles [A]

(USC-TAC) 213-749-5436

Los Angeles [A]

(USC-ARPA-TAC) [none known]

```
  San Diego [M]

(ACCAT-TAC)       619-225-1641, (R4), 619-225-6903,, V
                  619-225-6946 (R3)
                  ,, 619-223-2148,, V
                  619-226-7884, (R2)


  Santa Monica

(RAND-ARPA-TAC) [A]

                  213-393-9230
                  213-393-9237
                  213-393-9238
                  213-393-9239

(RAND2-MIL-TAC) [M]

                  [none known]



Colorado


  Denver Fed Ctr [M]

(USGS2-TAC)       303-232-0206,, 303-232-0206,, B/V


  Lowry Air Force Base [M]

(LOWRY-MIL-TAC)   [none known]
```

```
D.C. Washington


  Andrews AFB [M]

(AFSC-HQ-TAC)     301-967-7930, (R16), 301-967-7930, (R16), B
                  301-736-2990, (R4), 301-736-2990, (R4), B
                  301-736-2998, (R2), 301-736-2998, (R2), B
```

(PENTAGON-TAC)	202-553-0229, (R14), 202-553-0229, (R14), B

Florida

Eglin AFB [M]

(AFSC-AD-TAC)	904-882-8202,, 904-882-8202,, B/V
	904-882-8201,, 904-882-8201,, V

MacDill AFB [M]

(MACDILL-MIL-TAC)	[none known]

Naval Air Station - Jacksonville [M]

(JAX1-MIL-TAC)	[none known]

Naval Air Station - Orlando [M]

(ORLANDO-MIL-TAC)	[none known]

Georgia

Robins AFB [M]

(ROBINS-TAC)	912-926-2725,, 912-926-2725,, B/V
	912-926-2726
	912-926-3231
	912-926-3232
	912-926-2204,, 912-926-2204,, B/V

Hawaii

Camp H.M. Smith [M]

(HAWAII2-TAC)	808-487-5545,, 808-487-5545,, B

Illinois

Scott AFB [M]

(SCOTT-TAC)	[none known]
(SCOTT2-MIL-TAC)	[none known]

Kansas

Ft. Leavenworth [M]

(LVN-MIL-TAC)	913-651-7041, (R8), 913-651-7041, (R8), B

Louisiana

Navy Regional Data Automation Center [M]

(NORL-MIL-TAC)	504-944-7940,, 504-944-7940,, B 504-944-7948, (R2), 504-944-7948, (R2), B 504-944-7951, (R5), 504-944-7951, (R5), B 504-944-8702, (R8), 504-944-8702, (R8), B

Maryland

Aberdeen Proving Ground [M]

(BRL-TAC)	301-278-6916, (R4), 301-278-6916, (R4), B/V

Bethesda [M]

(DAVID-TAC)	202-227-3526, R16, 202-227-3526, R16, B/V

Patuxent River [M]

(PAX-RV-TAC)	301-863-4815,, 301-863-4815,, B/V 301-863-4816,, 301-863-4816,, B/V 301-863-5750, (R6), 301-863-5750, (R6), B/V

Silver Spring [M]

(WHITEOAK-MIL-TAC)

301-572-5960, R10, 301-572-5960, R10, B
301-572-5970, (R10), 301-572-5970, (R10), B

Massachuesetts

Hanscom AFB [M]

(AFGL-TAC)	617-861-3000, (R8), 617-861-3000, (R8), B 617-861-4965, (R8), 617-861-4965, (R8)

Cambridge

(BBN-MIL-TAC) [M]

[none known]

(BBN-ARPA-TAC) [A]

[no dialup capability]

(CCA-ARP-TAC) [A]

[none known]

```
(MIT-TAC) [A]      (617) 491-5669,, (617) 258-6224,, V
                   (617) 491-5708,, (617) 258-6225,, V
                   (617) 491-5734,, (617) 258-6227,, V
                   (617) 491-5819,, (617) 258-6248,, V
                   ,, (617) 491-5826
                   ,, (617) 491-5841
                   ,, (617) 491-5849
                   ,, (617) 491-6769
                   ,, (617) 491-6772
                   ,, (617) 491-6937
                   ,, (617) 258-6241
                   ,, (617) 258-6242
                   ,, (617) 258-6243


Michigan


  U.S. Army Tank Automotive Command (TACOM) - Warren [M]

(TACOM-TAC)        [none known]


Missouri


  St. Louis [M]

(STLA-TAC)         [none known]


Nebraska


  Offutt AFB [M]

(SAC1-MIL-TAC)     [none known]

(SAC2-MIL-TAC)     402-292-4638, (R10), 402-292-4638, (R10), B

(SAC-ARPA-TAC) [A]

                   402-294-2398,, 402-294-2398,, B
                   402-291-2018,, 402-291-2018,, B
                   402-292-7054,, 402-292-7054,, B
```

```
New Jersey

  Dover [M]

(ARDC-TAC)        201-724-6731,, 201-724-6731,, B/V
                  201-724-6732,, 201-724-6732,, B/V
                  201-724-6733,, 201-724-6733,, B/V
                  201-724-6734,, 201-724-6734,, B/V


  Fort Monmouth [M]

  (FTMONMOUTH1-MIL-TAC)

                  201-544-2052,, 201-544-2052,, B/V
                  201-544-2062,, 201-544-2062,, B/V
                  201-544-2072,, 201-544-2072,, B/V
                  201-544-2396,, 201-544-2396,, B/V
                  201-544-2430,, 201-544-2430,, B/V


  (FTMONMOUTH2-MIL-TAC)

                  201-544-4254, (R3), 201-544-2430,, B

                  ,, 201-544-2636,, B
                  ,, 201-544-2638,, B
                  201-544-2777,,,, B


New Mexico

  Albuquerque [M]

(AFWL-TAC)        [none known]


  White Sands [M]

(WSMR-TAC)        [no dialups; contact NSC for access]

                  Claude (Skeet) Steffey
                  ,, 505-678-1271
                  ,, FTS-898-1271
                  ,, AV-258-1271
```

```
<<>  G-File: The Official Phreakers Manual: PHREAK*.DOC     253
     G_PHREAK.WPS 11/20/90 11:29 AM
```

```
New York

  Griffiss AFB

(RADC-ARPA-TAC) [A]

                  [no dialup capability]

(RADC-TAC) [M]    315-339-4913, (R5)
                  315-337-2004,, 315-337-2004,, B/V
                  315-337-2005,, 315-337-2005,, B/V

315-330-2294      315-330-2294, (FTS), 952,, B/V

315-330-3587      315-330-3587, (FTS), 952,, B/V


North Carolina

  Ft. Bragg [A]

(BRAGG-ARPA-TAC)  919-396-1131, (R10), 919-396-1426, (R5), B/V
                  ,, 919-396-1491, (R8), B/V

  Ft. Bragg [M]

(BRAGG-MIL-TAC)   [none known]


Ohio

  Wright-Patterson AFB [M]
```

```
(WPAFB-TAC)        513-258-4218
                   513-258-4219
                   513-258-4987
                   513-258-4988
                   513-258-4989
                   513-258-4990

(WPAFB2-MIL-TAC)   513-257-2172, (R8), 513-257-2172, (R8), B
                   513-257-2690, (R8), 513-257-2690, (R8), B
                   513-257-3625, (R8), 513-257-3625, (R8), B
```

Oklahoma

  Tinker AFB [M]

```
(TINKER-MIL-TAC)   [none known]
```

Pennsylvania

  New Cumberland Army Depot [M]

```
(NCAD-MIL-TAC)     [none known]

(NCAD2-MIL-TAC)    [none known]
```

Texas

  Brooks AFB [M]

```
(BROOKS-AFB-TAC)   512-536-3081, (R6), 512-536-3081, (R6), B/V
```

  Richardson [A]

```
(COLLINS-TAC)      214-235-2131,, 214-235-2131,, B
                   214-235-2143,, 214-235-2143,, B
                   214-235-2178,, 214-235-2178,, B
```

```
                  214-235-2204,, 214-235-2204,, B
                  214-235-2251,, 214-235-2251,, B
                  214-235-2278,, 214-235-2278,, B


Utah


  Dugway Proving Ground [M]

(DUGWAY-MIL-TAC)  [none known]


  Salt Lake City (University of Utah) [A]

(UTAH-TAC)        801-581-3486, 801-581-3486,, B/V
```

```
Virginia


  Alexandria [M]

(DARCOM-TAC)      202-274-5300,, 202-274-5300,, B
                  202-274-5320, (R6), 202-274-5320, (R6), B


  Arlington

(ARPA1-MIL-TAC) [M]

                  [none known]

(ARPA2-MIL-TAC) [M]

                  [none known]

(ARPA3-TAC) [A]   [no dialup capability]


  Dahlgren [M]

(NSWC-TAC)        703-663-2162, (R8), 703-663-2162, (R8), B
```

```
  Langley Air Force Base [M]

(LANGLEY-MIL-TAC)

                  [none known]


  McLean [M]

(DDN-PMO-MIL-TAC)

                  [none known]

(MITRE-TAC) [M]   703-442-8020, (R15)
                  703-893-0330, R10, 703-893-0330, R10, B/V
```

```
  Norfolk [M]

(NORFOLK-MILTAC)  804-423-0241, (R2), 804-423-0241, (R2), B
                  804-423-0247, (R2), 804-423-0247, (R2), B
                  804-423-0346, (R4), 804-423-0346, (R4), B
                  804-423-0480,, 804-423-0480,, B
                  804-423-0486, (R2), 804-423-0486, (R2), B
                  804-423-0489,, 804-423-0489,, B
                  804-423-0570,, 804-423-0570,, B
                  804-423-0572, (R2), 804-423-0572, (R2), B
                  804-423-0577, (R2), 804-423-0577, (R2), B
                  804-423-0651,, 804-423-0651,, B
                  804-423-0654, (R3), 804-423-0654, (R3), B
                  804-423-0841, (R2), 804-423-0841, (R2), B
                  804-423-0845,, 804-423-0845,, B
                  804-423-0849,, 804-423-0849,, B
                  804-423-0858,, 804-423-0858,, B
                  804-423-0950,, 804-423-0950,, B
                  804-423-0952,, 804-423-0952,, B
                  804-423-0955, (R3), 804-423-0955, (R3), B
                  804-423-0959,, 804-423-0959,, B
```

Reston

(DCEC-ARPA-TAC) [A]

[no dialups available]

(DCEC-MIL-TAC) [M]

703-437-2892, (R5), 703-437-2928,, B
703-437-2925,, 703-437-2929,, B
703-437-2926
703-437-2927

Washington

Seattle [A]

(WASHINGTON-TAC) [no dialup capability]

Foreign

England [M]

(CROUGHTON-MIL-TAC)

[none known]

Germany [M]

(FRANKFURT-MIL-TAC) (M)

2311-5641, (R8), B

(RAMSTEIN2-MIL-TAC)

[none known]

Italy [M]

(AGNANO-MIL-TAC)

Japan [M]

(BUCKNER-MIL-TAC)

(ZAMA-MIL-TAC)

Korea [M]

(KOREA-TAC) (M)   264-4951, (R8),,,, B

Philippines [M]

(CLARK-MIL-TAC)

Spain [M]

(MILNET-TJN-TAC) [none known]

(ROTA-MIL-TAC)   [none known]

Notes

1. "(R10)" following phone number indicates a rotary with 10 lines.

2. For alternate phone numbers, FTS=Federal Telephone System.

3. (M)=Military DoD Telephone System.

4. [M] denotes a MILNET TAC and [A] denotes an ARPANET TAC.

5. "1200 Type" refers to the modem compatibility for 1200 baud only:

B/V	Bell and Vadic
B	Bell 212A only
V	Vadic 3400 only

6. This list is contained in the file NETINFO:TAC-PHONES.LIST at SRI-NIC.

Telco Test Numbers as of 5/16/85

Compiled and Updated by Shadow 2600

011-44-61-2468011	US dial tone then "When this system changes, this is the new dial tone you hear" (UK is changing dialtone)
201-226-0709	alternating tones, then "warble"

201-267-9922	sweep tone
201-267-9966	600 ohm termination

201-232-9924	(tone 1,2,5-beep, bleep; 9,#- 1200 baud static, beep, bleep; 6-tone, higher tone, bleep)
201-232-9959	tone 11 sec. silence, repeats...
201-233-9972	multitude of clicks
201-233-9974	busy 15 sec. then tone w/ clicks
201-241-9916	hissing with clicks
201-328-9971	1000 hrtz tone
201-376-9907	"is being checked for trouble. Please try again later"
201-464-9915	low tone 15 sec, silence
201-464-9916	low tone 2 sec, silence
201-464-9963	buzz
201-464-9974	busy 15 sec, low tone
201-543-9902	"If you'd like to make a call, hang up and try it again."
201-543-9903	"We're sorry, your call did not go through."
201-543-9904	"the number you have dialed requires a .20 cents deposit."
201-655-9900	"cannot be completed as dialed from the phone you are using"
201-769-0205	People's Express Reservation system
203-771-4920	telephone company employee newsline
207-866-4411	1000 hrtz tone
212-233-9980	(tone 1,2,3,*-tone, higher tone, bloop; 5-tone, bloop; 9,#-static,beep,bloop)
212-369-7003	"you have reached 212-369-7003 in zone 3" (?)

212-799-5017	ABC New York feed line
213-621-4141	telephone employee newsline
213-935-1111	sweep tone with echo at top of range (?)
215-489-0036	tone, bloop (1,2,5-tone bloop, 3,6,9-tone, higher tone,tone)
215-489-0040	"please check your instruction manual or call repair service for assistance"
215-489-0042	"if you like to make a call please hang up and try again"
215-489-0043	"We're sorry, your call did not go through."
215-489-0044	"The call you have made requires a 25 cent deposit"
215-489-0045	"You must first dial a 1 when dialing this number."
215-489-0074	LOUD tone, stops, repeats
215-489-0075	600 ohm termination (silence)
215-489-0078	tone, silence
215-489-0080	600 ohm termination
215-489-0097	tone, (lower pitched than -0078) silence (also at -0098)
215-489-0104	1000 hrtz tone
216-861-8300	tone, then higher tone
301-256-9987	1000 hertz
301-546-7777	"Due to Telephone Company facility trouble your call cannot be completed at this time"
301-725-9904	"deposit .20"
305-263-0000	repeating bloop (keypress 2 : slow reorder w/ bloops, clicks)
305-994-9963	pay fone instructions

305-994-9966	"telephone you are calling from is not in service"
312-222-9948	tone (keypress 1,2,3,6,7,*-tone, high tone, bleep, 4-tone,bloop,9, #-static,beep,bloop)
312-222-9954	"Test Center"
312-222-9990	clicks, ticking like
312-222-9996	LOUD tone, repeats
312-368-8000	Illinois Bell Communicator (employee newsline)
312-592-0000	tone (keypress 2222, then other digits, at re-order type * to restart) (?)
313-223-7223	telephone employee newsline
313-333-9981	LOUD tone, silence
313-333-9989	high tone (enter touchtones for a while, eventually get "metallic" echo, then 5-high pitched tone, random re-orders)
313-333-9990	beep, click repeats, with "winks"
313-333-9994	tone bloop (keypress in 2-tone,bloop, 3-tone, higher tone,tone, 9-static, beep,bloop)
313-333-9995	600 ohm termination (silence)
313-333-9996	weird siren/sweep tone, multi-frequency
313-430-4300	beep, beep, beep, then reorder
313-698-9998	sweep tone
314-247-5511	Southwestern Bell Telenews (employee newsline)
315-471-9934	"deposit 5 cents for next five minutes"
408-255-0081	(any two 2,4,8,0-tone)
408-294-6969	beep, click, computer voice repeats number
408-395-1110	(tone 2-bleep,glitch; 3-beep,higher

beep;#then number-loud tone,bleep)

408-738-8190	(tone 1,3,6,7,*-tone, high tone, tone;2-beep,cluck;9,#-static,tone,beep)
408-745-6060	high pitched tone, low tone then repeats
408-994-0044	tone end of loop
412-633-3333	telephone company employee newsline
414-628-0001	continuous tone
414-628-0002	continuous tone (higher pitched, sounds like muted dial)
414-628-0004	high pitched tone, bloop, silence
414-628-0006	brief very high tone (also -0007) (multiple keypresses of 2,5,8,0 tone repeats)
414-628-0010	loud tone, stops, repeats...
414-628-0011	loud tone, stops
414-628-0013	600 ohm termination (silence) (also -0017, two in an exchange?)
414-628-0014	continuous tone (sounds like weird dial), eventually stops
414-628-0015	LOUD tone, repeats
414-628-0028	"Your call cannot be completed as dialed
414-678-3511	Wisconsin Bell Newsline
414-781-0004	high tone, silence (keypress 2,5-beep,bleep, 3,6-beep,longbeep, bloop, 9-static,bloop)
415-284-1111	one sweep, then silence
415-327-0046	sweep tone
415-388-0037	tone,bloop (keypress 2-tone,bloop, 3-

	tone,high tone,tone, 9-static,beep,bloop)
415-472-0046	sweep w/ glitch at top
415-545-8800	Pacific Bell Newsline
415-467-0097	fast DTMF tones, keypress to repeat

415-777-0020	1000 hrtz tone
415-777-0037	tone, bloop (keypress 2-beep,bloop, 3,6-tone,higher tone, 9-static,beep,bloop)
415-777-0046	sweep tone with echo
415-777-0105	tone,bloop (keypress 2-beep,bleep, 3,6-tone, higher tone, tone,9-static,beep,bloop
415-826-0022	tone, click, tone (sounds like a busy)
415-994-0710	multitude of clicks
512-472-2181	"if you would like to make a call, please hang up and try again"
512-472-4263	garbled recording (?)
512-472-9833	"you must first dial a 1 or 0 before calling this number"
512-472-9936	"please check your instructions or call your business office for assistance"
512-472-9941	"insert 25 cents"
516-222-3825	LOUD tone
516-234-9914	New York Telephone Newsline
518-471-2272	New York Telephone Newsline
518-789-3299	weird busy, multitude of clicks
609-267-9966	busy with clicks in background
609-267-9967	600 ohm termination (silence)

609-267-9968	1000 hrtz tone
609-267-9971	LOUD tone, stops, repeats
609-267-9972	rings with clicks in background (also -9973 and -9974)
609-877-9924	high tone (tone in 1,2,5-tone, bloop; 3,6,*-tone, higher tone, bleep; #-static, beep, bleep)
609-877-9929	1000 hrz tone
617-553-9953	tone end of loop
617-890-9900	sweep tone
617-955-1111	telephone company employee newsline
619-748-0002	tone increases in pitch, silence, repeats in monotone
619-748-0003	sweep, repeat, hangs up
702-789-6711	Nevada Bell Newsline
713-354-0000	touch tone in #, then new #, then 5 - listed, 9 - unlisted)
713-482-3199	"We're sorry, all circuit are busy now."
713-652-5111	touch tones echo back "metallic", something about "drivers licence number" replys in a female recorded voice
717-255-5555	Bell of Pennsylvania "Inside Line" (employee newsline)
718-429-9900	"Please slide a valid credit card through the slot now"
800-221-5959	tone (# makes it ring)
800-228-8466	Sensaphone (tm) demo (time etc. (EST) (wait 7+ rings))

800-321-3048	non-connecting loop with 800-321-3049
800-321-3052	loop (don't know where other end is)
800-321-6366	Centagram's Voice Memo System (extension 100 for demo)
800-323-6321	tone, stops, bloop repeats
800-327-0000	"Announcement three, Dallas" (changes sometimes)
800-344-4001	non-connecting loop with 800-344-4002
800-524-0000	"Announcement 1 Atlanta"
800-554-5924	Cable News Network audio feed
800-824-8274	"Enter your password service code"

802-955-1111	telephone company newsline
808-533-4426	Hawaiian Telephone Newsline
816-391-1122	recorder (keypress 1-toggle on/off, 3-rewind, 4-stop, 7-play)
907-269-0955	tone (sounds like extender, doesn't take touch tone (?))
914-232-9901	"Daytona, New York DMS-100 verification"
914-268-9901	"Congers DMS 100 Verification"
914-268-9903	"your call cannot be completed as dialed"
914-268-9968	(keypress 2-high tone, 3-high, higher tone, 6,0-click, 7- hangs up, sometimes 0,#,*-harmony)
914-359-9901	repeats the number dialed ("914-359-9901")
914-359-9960	weird tone, stops, clicks, repeats
914-623-9968	(keypress 2,5-beep glitch, 3,6-tone highertone)

916-480-8000 Pacific Bell Newsline

What a TSPS Console Looks Like

```
---------- non/coin ---------- ------ coin ----- -- hotel --

┌────┐┌────┐┌────┐┌────┐┌────┐┌────┐┌────┐┌────┐┌────┐┌────┐
│vfy ││over││scrn││inwd││emer││sta ││0+  ││dial││sta ││0+  │
│dial││post││tone││sta ││0+  ││dial││qst ││    ││    ││    │
└────┘└────┘└────┘└────┘└────┘└────┘└────┘└────┘└────┘└────┘
```

```
-------------- outgoing trunks - ring release --------------

┌────┐┌────┐┌────┐┌────┐┌────┐┌────┐┌────┐┌────┐┌────┐┌────┐
│da  ││r&r ││swb ││ogt ││back││fwd ││call││t&c ││nfy ││chg │
│    ││    ││    ││    ││    ││    ││    ││    ││    ││due │
└────┘└────┘└────┘└────┘└────┘└────┘└────┘└────┘└────┘└────┘

┌────┐┌────┐┌────┐┌────┐┌────┐┌────┐┌────┐┌────┐┌────┐┌────┐
│key ││back││fwd ││sr  ││make││mtce││pos ││back││    ││    │
│clg ││    ││    ││    ││busy││trfr││    ││    ││    ││    │
└────┘└────┘└────┘└────┘└────┘└────┘└────┘└────┘└────┘└────┘

           ---------------- ama -----------------

            ┌────┐┌────┐┌────┐┌────┐┌────┐┌────┐
station <-> │paid││col ││spl ││spl ││auto││ddd │
            │    ││    ││clg ││cld ││col ││    │
            └────┘└────┘└────┘└────┘└────┘└────┘

            ┌────┐┌────┐┌────┐┌────┐      ┌────┐
person <--> │paid││col ││spl ││spl │      │no  │
```

```
│    │ │    │ │clg │ │cld │       │ama │
└────┘ └────┘ └────┘ └────┘       └────┘

┌────┐       ┌────┐       ┌────┐
│clg │       │clg │       │clg │
│    │       │    │       │    │
└────┘       └────┘       └────┘
```

Box Plans

Hmm... I wonder! This is still under construction (Ha Ha).

The Infinity Transmitter

Typed by the Ghost Wind

From the book Build Your Own Laser, Phaser, Ion Ray Gun & Other Working Space-Age Projects by Robert Iannini (Tab Books, Inc.)

Description

Briefly, the Infinity Transmitter is a device which activates a microphone via a phone call. It is plugged into the phone line, and when the phone rings, it will immediately intercept the ring and broadcast into the phone any sound that is in the room. This device was originally made by Information Unlimited, and had a touch tone decoder to prevent all who did not know the code from being able to use the phone in its normal way. This version, however, will activate the microphone for anyone who calls while it is in operation.

Note It is illegal to use this device to try to bug someone.
It is also pretty stupid because they are fairly noticeable.

Parts List

Pretend that uF means micro Farad, cap= capacitor

Part	#	Description
R1,4,8	3	390 k 1/4 watt resistor
R2	1	5.6 M 1/4 watt resistor
R3,5,6	3	6.8 k 1/4 watt resistor
R7/S1	1	5 k pot/switch
R9,16	2	100 k 1/4 watt resistor
R10	1	2.2 k 1/4 watt resistor
R13,18	2	1 k 1/4 watt resistor
R14	1	470 ohm 1/4 watt resistor
R15	1	10 k 1/4 watt resistor
R17	1	1 M 1/4 watt resistor
C1	1	.05 uF/25 V disc cap
C2,3,5,6,7	5	1 uF 50 V electrolytic cap or tant **
C4,11,12	3	.01 uF/50 V disc cap
C8,10	2	100 uF @ 25 V electrolytic cap
C9	1	5 uF @ 150 V electrolytic cap
C13	1	10 uF @ 25 V electrolytic cap
TM1	1	555 timer dip
A1	1	CA3018 amp array in can
Q1,2	2	PN2222 npn sil transistor
Q3	1	D4OD5 npn pwr tab transistor

D1,2	2	50 V 1 amp react. 1N4002
T1	1	1.5 k/500 matching transformer
M1	1	large crystal microphone
J1	1	Phono jack optional for sense output
WR3	24"	#24 red and black hook up wire
WR4	24"	#24 black hook up wire
CL3,4	2	Alligator clips
CL1,2	2	6" battery snap clips
PB1	1	1 3/4x4 1/2x.1 perfboard
CA1	1	5 1/4x3x2 1/8 grey enclosure fab
WR15	12"	#24 buss wire
KN1	1	small plastic knob
BU1	1	small clamp bushing
B1,2	2	9 volt transistor battery or 9V ni-cad

** (preferably non-polarized)

Circuit Operation

Not being the most technical guy in the world, and not being very good at electronics (yet), I'm just repeating what Mr. Iannini's said about the circuit operation. The Transmitter consists of a high grain amplifier fed into the telephone lines via transformer. The circuit is initiated by the action of a voltage transient pulse occurring across the phone line at the instant the telephone circuit is made (the ring, in other words). This transient immediately triggers a timer whose output pin 3 goes positive, turning on transistors Q2 and Q3. Timer TM1 now remains in this state for a period depending on the values of R17 and C13 (usually about 10 seconds for the values shown). When Q3 is turned on by the timer, a simulated "off hook" condition is created by the switching action of Q3 connecting the 500 ohm winding of the transformer directly across the phone lines.

Simultaneously, Q2 clamps the ground of A1, amplifier, and Q1, output transistor, to the negative return of B1,B2, therefore enabling this amplifier section. Note that B2 is always required by supplying quiescent power to TM1 during normal conditions. System is off/on controlled by S1 (switch).

A crystal mike picks up the sounds that are fed to the first two transistors of the A1 array connected as an emitter follower driving the remaining two transistors as cascaded common emitters. Output of the array now drives Q1 capacitively coupled to the 1500 ohm winding of T1. R7 controls the pick up sensitivity of the system.

Diode D1 is forward biased at the instant of connection and essentially applies a negative pulse at pin 2 of TM1, initiating the cycle. D2 clamps any high positive pulses. C9 DC-isolates and desensitizes the circuit. The system described should operate when any incoming call is made without ringing the phone.

Schematic Diagram

Because this is text, this doesn't look too hot. Please use a little imagination! I will hopefully get a graphics drawing of this out as soon as I can on a Fontrix graffile.

To be able to see what everything is, this character: | should appear as a horizontal bar. I did this on a][e using a][e 80 column card, so I'm sorry if it looks kinda weird to you.

Symbols

```
    -/\/\/  resistor           _/ _  switch

    -|!|!-  battery            -|(-  capacitor (electrolytic)

     -||-   capacitor (disc)     |<  diode

                             _    _
(c)  > (e)  transistor        )||(   transformer
  \_/                         )||(
   |(b)                      _)||(_

   ._____.  chip
   !_____! (chips are easy to recognize!)
```

Dots imply a connection between wires. No dot, no connection. ie.: _!_ means a connection while _|_ means no connection.

```
._________________________to GREEN wire phone line
|
| .______________________to RED wire phone line
| |
| | ._________(M1)___________.
| | |                        |
| | |           R1           |
| | !__________/\/\/_________!
| | |                      _!_ C1
| | |this wire is the amp   ___
| | |<=ground                |              R2
| | |                        !____________/\/\/_________.
| | |                  .____!____.                     |
| | !__________________!4   9  11!_____________________!
| | |                  |         |                     |
| | !__________________!7      12._____________________!
| | |                  |   A1    |          R3         |
| | !__________________!10    _*8!___.____/\/\/________! ^
| | |                  |     /   |   |                 | |
| | |    C4            |    <    |   \                 |2ma
| | !____||______.     |    |    |   /R4          B1 +
| | |    ||      |     |    |    |   \               |!|!
| | |     R7     |  C2 |    >    |   /                 |
| | !____/\/\/___!__)|__!8*_/     |   |             S1  |
| | |     ^            |        6!___!       neg<__/.__!
| | |     |     C3     |         |   | C5   return     |
| | |     !_____|(___.__!3        |   '-|(-|            |
| | |               |  |    5   1!________!            |
| | |               \  !____.____!        |         B2|!|!
| | !________.    R8 /      |             |            +
| |         |       \       |             |     R6     |3ma
| |         |       !_______!_____________|____/\/\/___! |
| |         |    R5         |             |            | v
| |         !__/\/\/________|_____________!            |
| |         |               |                          |
| |         |               |                          |
| |         |            C6 |                          |
| |         |          |-)|-'      R9                  |
| |         |          !__________/\/\/_______.        |
| |         |          |                      |        |
| |         |      Q1 _!_                     |   R10  |
| |         !_________/ \_____________________!_/\/\/__!
| |         |                                 |        |
| |         |                                 |        |
| |         |       C8                        |        |
| |         !_______)|________________________|________!
| |         !                                 |        |
| |        _/                                 |        |
| |   ----|                                   |        |
| |   |   |                                   |        |
| |   |   |                                   |        |
| |   |   |                                   |        |
| |   |   |                                   |        |
| |   |   !_______.                           |        |
| |   |           |                            |        |
| |   !____.      |                            |        |
| |        |      |                            |        |
| !____.   |      |                .___________!        |
|      |   |      |                |                    |
|      |   |      |                |                    |
|      |   |      |                | C7                 |
|      |   |      |                '-|(-|               |
|      |___|______!______.T1.___________|               |
|          |      | 1500 )||( 500                       |
|          |      |   ohm )||( ohm                       |
|          |      !_____.)||(.__.                       |
|          |      |             |                       |
|          |      |          .__!                       |
|          |      |          >                          |
|          |      |        |/                           |
|          |      |    +---|   Q3                       |
|          |      |    |   |\                           |
!__________|______|____|_____!__. D1   C9               |
           |      |    |        '-|<---|(-------|       |
      .____!      |    |                        |       |
      |           |    |                        |       |
      | .________!    |                        |       |
      | |              |                        |       |
      \ |       .______!            C11         |       |
      / |       |               .___||__________!       |
  R13 \ |       |               |   ||          |       |
      / |       |               |               |       |
      \ !___.___|_______________!               |       |
      | |   |   |               |     R16       |  R15  |
      | v   |   |               !___/\/\/\______!_/\/\/_!
      | neg |   |               |    D2         |       |
      | ret |   |               !_____|<________!       |
      |  B1 |   \               |               |       |
      |  B2 |   /               |    .__________!_.     |
      |     |   \R14            |C12 |   TM1    2 |     |
      |     |   /               !_||_!5          4!_____!
      |     |   \               | || |            |     |
      |     |   |               !____!1          8!_____!
      |     |   |               |    |     7 6 3  |     |
      |     |   |               |    !_____._.__._.     |
      |     |   |               |          | |  |       |
      |     |   |               |   C13    | |  |  R17  |
      |     |   |               !___)|_____!_!__|_/\/\/_!
      |     |   |               |               |       |
      !_____|___!_______________|_______________!       |
            |   |               |                       |
            |   \               |          C10          |
            |   /R18            !__________)|___________!
            |   \
            |   /
            |   |
```

```
            !___O J1
              sense output
```

Construction Notes

Because the damned book just gave a picture instead of step by step instructions, and I'll try to give you as much help as possible. Note that all the parts that you will be using are clearly labeled in the schematic. The perfboard, knobs, 'gator clips, etc are optional. I do strongly suggest that you do use the board! It will make wiring the components up much much easier than if you don't use it.

The knob you can use to control the pot (R7). R7 is used to tune the IT so that is sounds ok over the phone. (You get to determine what sounds good) By changing the value of C13, you can change the amount of time that the circuit will stay open (it cannot detect a hang up, so it works on a timer.) A value of 100 micro Farads will increase the time by about 10 times.

The switch (S1) determines whether or not the unit is operational. Closed is on. Open is off. The negative return is the negative terminals of the battery! The batteries will look something like this when hooked up:

```
     <-v_____.   .______.    ._____.   .____->
             |   |      |    |     |   |
           __!___!__    |    |   __!___!__
           | +   - |    !_/ _!   | +   - |
           |       |  switch ^   |       |
           | 9volts|         |   | 9volts|
           !_______! neg return  !_______!
```

To hook this up to the phone line, there are three ways, depending upon what type of jack you have. If it is the old type (non modular) then you can just open up the wall plate and connect the wires from the transmitter directly to the terminals of the phone.

If you have a modular jack with four prongs, attach the red to the negative prong (don't ask me which is which! I don't have that type of jack... I've only seen them in stores), and the green to the positive prong, and plug in. Try not to shock yourself...

If you have the clip-in type jack, get double male extension cord (one with a clip on each end), and chop off one clip. Get a sharp knife and splice off the grey protective material. You should see four wires, including one green and one red. You attach the appropriate wires from the IT to these two, and plug the other end into the wall.

Getting the IT to Work

If you happen to have a problem, you should attempt to do the following (these are common sense rules!) Make sure that you have the polarity of all the capacitors right (if you used polarized capacitors, that is). Make sure that all the soldering is done well and has not short circuited something accidently (like if you have a glob touching two wires which should not be touching.) Check for other short circuits. Check to see if the battery is in right. Check to make sure the switch is closed.

If it still doesn't work, drop me a line on one of the Maryland or Virginia BBSs and I'll try to help you out.

The Sense Output

Somehow or other, it is possible to hook something else up to this and activate it by phone (like an alarm, flashing lights, etc.)

As of this writing, I have not tried to make one of these, but I will. If you actually get it working, leave me a note somewhere.

I sure hope all you people appreciate this.

<<> G-File: The Official Phreakers Manual: PHREAK*.DOC   274
G_PHREAK.WPS 11/20/90 11:29 AM

Silver Box
An Alternate Method of Construction

By the Lock Lifter
85/1/25

Parts & Equipment

1. Pocket tone dialer (radio shack cat. No. 43-138)
2. Single pole double throw switch (toggle, the smaller the better)
3. Soldering iron

This modification will allow the production of a,b,c,&d tones. When you flip the switch the 3,6,9,&# keys will become a,b,c,&d respectively. The ic inside the dialer is capable of making these tones already, all we must do is connect it fully. This mod can also be made to many electronic fones that contain a dtmf tone encoding ic. This chip can be identified by the number 5089 or s2559 or mk5380 or tcm5087n. Pin 9 of these chips is the fourth column keypad input while pin 5 is the third column. Now on with the construction.

1. Remove the battery cover, batteries, and the small screw. The case should now pop open with a little pressure.

2. Open the case so that the half containing the speaker and the batteries is on your left with the batteries on the bottom. You should now be looking at the back of 2 printed circuit boards.

3. Find the two rows of solder beads where the ic is connected. The upper left pin of the 2 rows should have no solder on it. This is pin 9 of the ic.

4. Attach a short wire to pin 9.

5. See the 8 gold wires going to the key pad? Unsolder the one 4th from the left and connect it to a short wire.

6. Solder a short wire into the now vacant hole in the keypad pcb.

7. Melt or drill a round hole in the plastic case for the switch. The best place for this is opposite the small pcb containing the l.e.d.

8. Insert the switch and screw it in place.

9. Attach the wire from the keypad pcb to the center of the switch. Attach the other two wires to the other two poles of the switch. Just close the case, put back in the screw and batteries.

The switch will now allow the 3rd column keys to produce both 3rd and fourth column tones. Have phun.

```
<<>  G-File: The Official Phreakers Manual: PHREAK*.DOC     276
     G_PHREAK.WPS 11/20/90 11:29 AM
```