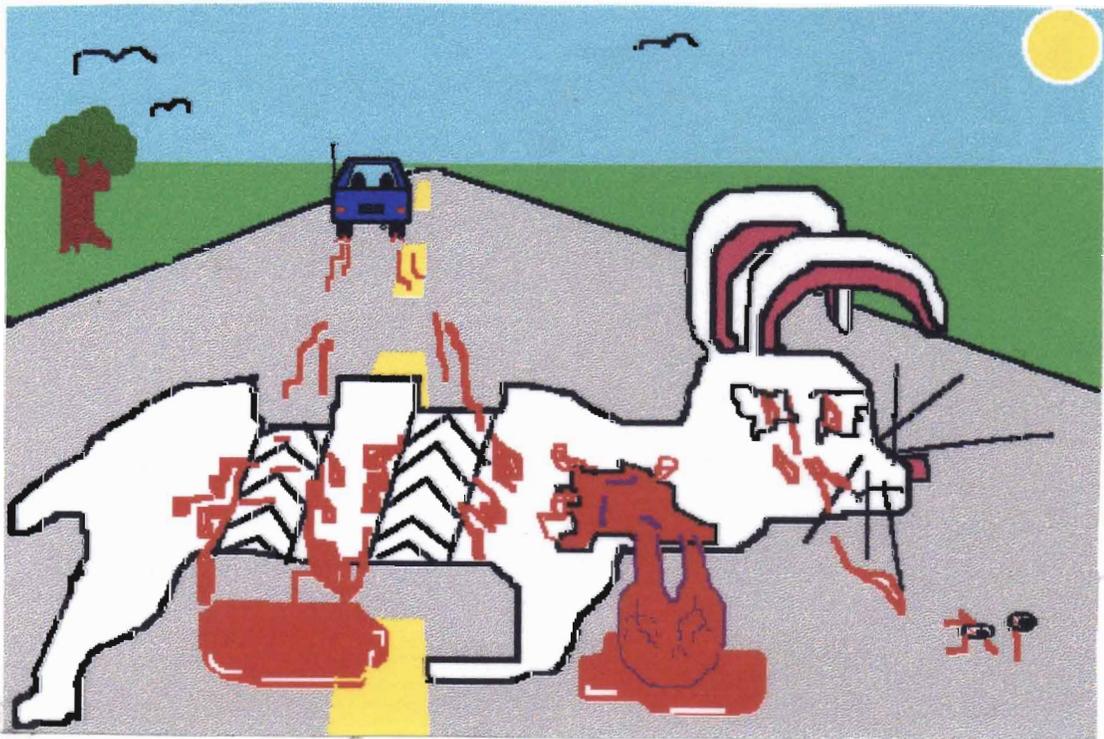


CYBER ZINE

ISSUE #8

\$1.50



KNOCKED OUT BY THE MONOPOLY!

!FOR INFORMATIONAL USE ONLY!

COVER BY FOTON FANTOM

EXPLOSIVES, BOMBS, AND OTHER NEAT STUFF

Soda Bomb: A very loud noise maker can be made using pool chlorine, sugar, water, and a two-liter soda bottle. First, go to a store that sells pool supplies. Buy a small bag of chlorine powder. Make sure it is at least 75% sodium hypochlorate. Just look on the back in the ingredients list, it will tell you. Next, get a two-liter soda bottle, a bag of sugar a some water.

Go into your backyard and pour about 4 oz. of pool chlorine into the soda bottle. (This would be $\frac{1}{4}$ of a one pound bag) The amount doesn't have to be exact. After that pour an equal amount of sugar on top of the chlorine. Again, the amount doesn't have to be exact. Now for the fun part. Slowly pour the water into the bottle. Be careful not to shake the bottle to much or it will explode in your face. The amount of water put into the bottle will vary with altitude, humidity, gravitational forces, and other natural things so you may have to experiment a little bit. After you do put the water in, put the cap on tightly and through it into your neighbors yard. What actually happens is chlorine and hydrogen are released in the chemical reaction. These build up in the soda bottle until it explodes. It will sound about as loud as an M-80, and will even leave a little crater. The only draw back is the releasing of chlorine into the air. Not only does it destroy the ozone layer, but it also hugs the ground and gets blown around by the wind, and if you don't already know chlorine will kill you. STAY AWAY FROM IT. Have fun.

-Cyber 'Zine staff

Stink Bomb: Put some Drano and egg whites into a glass jar and mix them up a little. Place the jar (with the cap on) into direct sunlight on a hot day. To use it, go into school, a store, or where ever and splash it all over. This stuff will get them running!

Mercury Fulminate: Mercury fulminate is used in the making of detenators. (they set off bigger explosives) It is easy to make, but you must be careful.

Materials Required

Nitric Acid- 90% concentrated
Mercury- from thermometers and switches
Ethyl alcohol- also called grain
Filtering materials- paper towels
Teaspoons- your ma
Heat source- stove
Wood stick- a tree
Clean water- not the Fox
Glass container- just about everywhere
Tape and a Syringe- you druggie

Next Page.....))))))

Carrier Access Code

~~~~~

The carrier access code is a set of digits dialed by an end user to access the particular inter-exchange carrier (IC) to be used for a call, other than the IC to which the customer has pre-subscribed. For Feature Group B type of access these codes are in the form of - 950-WXXX (where W=0 or 1 and XXX is the Carrier Identification Code-CIC). (CIC is the last three digits of the carrier access code that designate a specific inter-exchange carrier. For Feature Group D (equal access) they are in the form of 10XXX (where XXX=CIC). After these codes have been dialed and the customer has received dial tone from the IC, the number being called is dialed.

## Feature/Function Access Code

~~~~~

A code, dialed using a keypad such as is on a non-rotary telephone (touch-tone), of the form *XX or XX, currently used by end users for control and access to custom calling features. Future applications *XX(X) may be include access to special features, functions, or services provided by interLATA (inter-exchange) carriers (ICs) after a carrier access code has been dialed.

Feature Groups (FG) A, B, C, and D

~~~~~

Access arrangements provided by local exchange carriers to inter-exchange carriers for access to the local network. FGA is a line side connection whose use requires customers to dial between 17 and 24 digits to complete a call. FGB is a trunk side connection where the customer dials 950-WXXX (see Carrier Access Codes) to reach a specific inter-exchange carrier. When the customer gets dial tone from the carrier, he or she dials a personal identification code and the number of the person being called. FGC is the form of interconnection offered to AT&T after divestiture (and was still offered to AT&T after divestiture until FGD equal access was available in an office) connecting the trunk side of the local central office to the inter-exchange carrier's Point of Termination (POT). It requires only the digit "1" to be divided to reach AT&T and the 7 or 10 digits to complete the call. When equal access arrangements are available, all inter-exchange carriers are offered FGD, which makes it possible for customers to dial only "1" to reach the carrier of their predetermined choice whether that is AT&T or not, and then 7 or 10 digits to reach the party being called. FGD is an end office trunk side connection connecting the inter-exchange carrier's POT to the end office, either directly or through a tandem switch. (pre-subscription- a local exchange company (LEC) tariffed service that permits each customer served from an equal access end office switching system to route automatically, without the use of access codes, all the customer's interLATA communications to one interLATA carrier (IC) of the customer choice.

OPENING HANDCUFFS  
\*\*\*\*\*

The handcuff lock is one of the oldest and simplest locks around. There are hundreds of different methods to open them. Here are just a few.

The key used to open handcuffs is very simple itself. It consists of a small handle, a shaft with a hole in the end, and a small knob that sticks out of the shaft on the end of the key. That knob is what actually opens the handcuff. The hole is there to prevent anyone from sticking something in the keyway to open the lock. All the keys to different brands of handcuffs are very similar. The key from one brand may open another brand. Go to a police supply store, or borrow a good pair of handcuffs and practice a lot. If you do manage to get a key, cut off part of the handle. This will make it very concealable, and yet it will still make it easy to turn.

Picking handcuff locks is also possible. All that prevents some handcuffs from opening is a small ratchet wheel, and a inter-locking finger mechanism. By using a narrow piece of metal as a shim, you can slip it under the finger that prevents the ratchet wheel from turning. You can now pull the cuff open without having the finger interfere with the ratchet wheel.

Another method is using a home made key. The metal refill barrel of some ball point pens fits over the post in the handcuff keyway. Just slit the top of it and bend it up a little bit, forming the same knob that is on a real key. Different sizes of this improvised key could be very handy. You could conceal it inside a pen case. No one would ever think it was a pick.

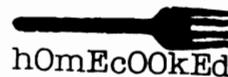
---

FCC License for the city of Green Bay

Radio Service- YP Trunked public service/special emergency  
Frequency advisory number- WNKD419  
Number of vehicular units- 240  
Number of portable units- 220  
Number of aircraft units- 0  
Number of marine units- 0  
Number of pager units- 0

FREQUENCIES  
\*\*\*\*\*

856.2125 MHz                    150 watt output                    (base)  
857.2125 MHz                    "  
858.2125 MHz                    "  
859.2125 MHz                    "  
860.2125 MHz                    "  
811.2125 MHz  
812.2125 MHz  
813.2125 MHz  
814.2125 MHz  
815.2125 MHz



Transmitter street address- 1530 N. Bylsby Av. Green Bay  
Control point- 307 S. Adams St.  
Control point phone number- 436-3800



YOUR LINK TO A BETTER *MANAGED* POLY

## Dead Drops

~~~~~

Dead drops are places where spies can leave messages for other agents to receive. Spies don't communicate in person or over telephone lines for fear that they are being monitored. Since their identity is preserved by never coming in contact with another agent, their cover is never blown.

First, you must choose the location of your dead drop. This must be in a place where there isn't a lot of people, but yet, not in a too remote location. It should also provide some type of protection as you drop off and pick up messages.

Now you are ready to use your dead drop. You must hide the message in some type of container that will protect it from the weather, and people walking by. You should at least have two or three dead drops. This will allow you to drop back, and deliver messages to another dead drop if one of the locations is risky. If the dead drop is discovered by the enemy, you will have to stop using it. If the dead drop is discovered by the enemy, you can leave false information in it to set them up. They will think that the information is legitimate, and will act on it. If you leave a message that a secret meeting is coming up, you could stake out the area and ambush them.

If you are using more than one dead drop, you will have to leave clues telling your agent which drop to pick up, or leave the information at. These can be chalk marks, stones, or any thing that wouldn't look out of place. The marks should be left at a place where your agent will be able to see them easily. Example: Two vertical chalk marks at the main entrance to the Ameritech central office could mean that he should use dead drop number two. Good communication among all your agents will insure that your information is secure. You can also leave marks telling if a dead drop was discovered or if your being followed.

After you reach the dead drop site, check to make sure no one followed you or that there is no people close by. By walking across large fields and uncrowded streets you can see if any one is following you. Also, looking in the windows of stores you can check if any one is behind you. Once you reach the dead drop site, pretend to stop and tie your shoe, or drop some change. This will cover your actions as you pick up the message container.

Notes

- cutting the bottom off of pop cans makes a nice, large area to put a message in, and they don't look suspicious lying around in bushes.
- sprinkling a few grains of salt into your message and then folding it carefully will tell you if someone opened your message without you knowing it.
- you can also put a drop of glue on a corner and seal the message. When someone unfolds the message the seal is broke.
- Russians have hundreds of dead drops in Moscow. People have been whisked away to the police department, only to learn that they were standing too close to an active Russian dead drop.

Use of CICS

~~~~~

If multi is down. you can still access the system by logging onto CICS. To logon from the Ameritech Warning System screen. You will need to type:

LOG ACICPC11

-----  
This will get you to the screen that will ask you for user i.d. and password. Enter those two items and you will have access. If you are "Clocked Out" on the bottom of any screen, your user i.d. is frozen and this method of sign-on is not available

=====

## CALLER ID

-----  
Caller ID is not yet available for Wisconsin customers. Ameritech hopes to introduce Caller ID some time during winter of 1993.

Caller ID is an optional service which allows a customer to identify the telephone number from where an incoming call is originating. The number is displayed on a CPE device attached to the Caller ID subscribers telephone line. Caller ID is one of the advanced custom calling services.

## FREE Call Blocking Option

-----  
When placing an outgoing call, Ameritech customers served by an SS7 equipped central office face the possibility of having their phone number displayed to a Caller ID subscriber in another state.

To block delivery of a telephone number, the person placing the call must:

1. Dial \*67 from a Touch-Tone phone (1167 from rotary) PRIOR to placing the call.
2. Will hear stutter dial tone; wait until you hear a steady dial tone.
3. Dial the number you wish to reach.

## Miscellaneous:

- There is no charge for the call blocking option.
- Each time a call is placed and the customer wishes to block delivery, they must dial \*67. The block is in effect only for that call.
- Each SS7 central office is automatically equipped with call blocking.
- Pay phones will not be equipped with the call blocking option.

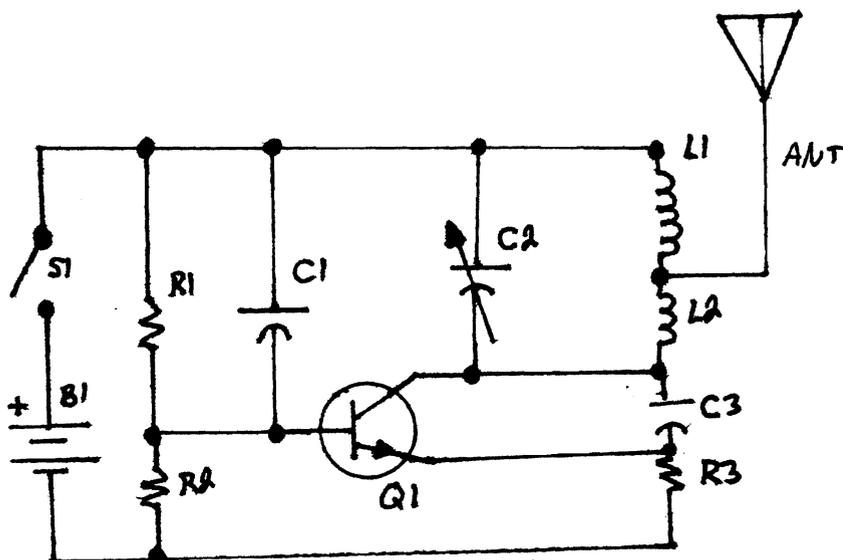
PROPRIETARY - BELLCORE AND AUTHORIZED CLIENTS ONLY

This document contains proprietary information that shall be distributed or routed only within Bellcore and its authorized clients, except with written permission of Bellcore.

How to use it:

Turn on your FM radio or T.V. and adjust the adjusting screw on the variable capacitor C2. Use a non-conductive tuning tool or piece of plastic to tune the capacitor. Slowly turn the adjusting screw until you see or hear a disturbance in the television or radio. Then with careful adjustment you will completely blank out reception. If you do not blank out reception, slightly separate the turns of the wire in the two coils L1 and L2. Try adjusting the capacitor again. Each station requires a different setting of the variable capacitor

To use this circuit as a FM transmitter, connect a 8 ohm speaker to the ground end of resistors R3 and R2. Open the ground lead of R3 from the PC board with your soldering iron. Solder a lead from the speaker to the lead of resistor R3. Insert the other speaker lead into the PC board where the R3 lead was and solder in place to the PC board. Use C2 for rough adjustment and the tuning knob on the radio for fine adjustment, then speak into the speaker and hear yourself on the radio.

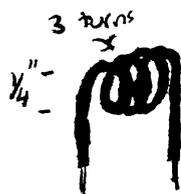


PARTS LIST

- R3 - 1K $\Omega$  resistor  $\frac{1}{4}$  watt, 5%
- R2 - 10 K $\Omega$  resistor  $\frac{1}{4}$  watt, 5%
- R1 - 82 K $\Omega$  resistor  $\frac{1}{4}$  watt, 5%
- C3 - 10pfd Capacitor
- C2 - 8-80 pfd Variable Capacitor
- C1 - .001 $\mu$ fd Capacitor
- Q1 - 2N3904 Transistor
- L1, L2 - 3 turn Coil
- S1 - Switch, SPST

B1 - 9 volt battery

ANT - Wire, 4 inch



The Coils should look like this. You will probably have to make four turns. Use solid wire about twice as thick as the leads on the resistors.

Here are some of the acronyms that you might encounter in the phone company's maintenance and record keeping systems.

1. Loop Maintenance Operations System (LMOS)

The LMOS system mechanizes the administration support of Plain Old Telephone Service (POTS)- like trouble reports. Starting with Repair Service Answering, Automated Screening and continuing through field dispatch and completion. There are several systems related to the LMOS system that comprise the Automated Repair Service Bureau environment.

2. Mechanized Loop Test (MLT)

MLT is a mechanized test system that provides mechanized testing of the local loop circuits in conjunction with the central office switch. It is directly related to LMOS for circuit data and communication. In today's environment, there are two versions of MLT, MLT-1, which is the older of the two systems and MLT-2.

3. Cable Repair and Analysis System (CRAS)

The CRAS system is a cable trouble report analysis system. With links to LMOS host and MTR, CRAS collects data and allows the end-user to request analysis data to determine cable repair trends.

4. Automated Cable Expertise (ACE)

ACE uses data collected by CRAS to analyze the completed cable trouble reports in an effort to determine potential problems and chronic areas in the local loop plant.

5. Voice Customer Access System (VCAS)

VCAS is a PC voice interface system that allows customers to enter trouble reports directly into the LMOS system. It also allows customers to check the status of previously entered trouble reports.

6. Ameritech Service Management System (ASMS)

ASMS is a Bellcore developed software application that allows customers to access LMOS and Circuit Installation and Maintenance Package (CIMAP) to enter and obtain status on trouble reports. It also allows customers to perform electronic test and request traffic management reports.

7. Craft Access System (CAS)

The CAS system allows field technicians to access LMOS to receive and close trouble report data via hand held terminals. Field technicians are also able to request MLT test request through the LMOS work manager.

8. Mechanized Trouble Analysis System (MTAS)

MTAS was developed by a small software company called Spencer and Spencer, and is used to collect completed trouble report information from the LMOS host and provide internal measurement reports. The MTAS software is owned by Ameritech and resides on mainframe computers.

9. Predictor

Predictor is a system that collects data from various systems where preset thresholds are invoked to determine probable areas of trouble in the outside plant environment. Predictor is part of the ARSB system.

10. Circuit Installation and Maintenance Package (CIMAP)

CIMAP mechanizes the administration support of the Installation and Maintenance for Special Services. Message Trunks and Interoffices Facilities. The CIMAP system consists of two primary software modules. CIMAP/SSC (Special Service Center) mechanizes work flows, document access and transfer processes for installation and creates, distributes, tracks, and logs trouble reports for maintenance.

11. Generic Dispatch System (GDS)

GDS mechanizes the administration support for the installation and maintenance for POTS and Special Services. It is inter-related to the CIMAP product line and forms the basis for Bellcore Work and Force Administration (WFA) system.

12. Trunk Integrated Record Keeping System (TIRKS)

For operations, TIRKS is used as the source for obtaining the WORD document for provisioning via an interface to CIMAP.

13. Switched Access Remote Test System (SARTS)

SARTS is a remote test system that permits testing of special service circuits from the SSC without assistance of technicians in the central offices.

14. Mechanized Time Recording (MTR)

MTR is the system used to report hours and minutes associated with work function codes of the employees. CIMAP and GDS-SSDAC have interface to the MTR system.

15. Service Order Analysis and Control (SOAC)

The SOAC interface system is a part of Bellcore's FACS system and serves as an interface between the local Service Order Processor (SOP) and GDS. It receives the service order data from the SOP and automatically queries LFACS and COSMOS for the cable and pair and office equipment facilities.

16. CAS/Gateway

The CAS/Gateway application via a component of the CAS system and is currently used to obtain trouble report history information from the LMOS host by the field technicians. It is also used to obtain cable and pair information from LFACS and planning is underway to provide access to GDS from the hand held terminal.

17. Service Order Processor (SOP)

The SOP issues the service orders to Operations Support Systems and accept completion information which is subsequently distributed to the billing system. GDS will automatically enter completion statistics to the SOP via generic SOP interface.

18. Automatic Line Record Update (ALRU)

The ALRU process takes completed service order data via computer tapes and reformats the information. It then uploads the information into the LMOS host which establishes a permanent line record for the circuit in the LMOS database.

19. Mizar (Versanet)

The Mizar system is a memory administration system used by the RCMAC to translate line service order data into recent change messages in an ESS (Electronic Switching System) office. The system automatically generates recent change messages and updates switches on the appropriate date as well as making switch changes for residential service without the need for physical wire changes.

Versanet was the Illinois version of Mizar and was replaced in '93

20. OPS/INE

The OPS/INE system mechanically converts and transmits TIRKS provisioning data to Intelligent Network Elements (INE). All provisioning functions are automatic and flexibly driven by date and time. INE memories are permanently stored in OPS/INE databases from which failed INE's can be restored.

All of these systems are inter-related in the maintenance system.

