The Black Book.

issue #5

Editor of the Month

m0ther

with some help from

mad d0g

volume # 1

For Informational Purposes Only (maybe)

T-1 SIGNALING AND ERROR DETECTION

Digital transmission over long distances saw commercial application in the early 1960's with T-1. T-1 is a way of time-multiplexing 24 voice communication channels over a single copper wire pair. Each voice frequency (VF) channel is sampled, then converted to an eight bit digital word that represents the channel signal at that moment. Each channel is sampled sequentially, yielding 192 bits (24 channels X 8 bits per channel). A 193rd bit is added to identify the beginning of another frame. Frames are gathered 8000 times a second giving T-1 a transmission speed of 1.54Mbps (193 bits per frame X 8000 frames per second). Standards for pulse amplitude, width, repetition rate, consecutive zero bits, and ratios of ones to zeros, is called Digital Signal at the first level (DS-1). The 193rd bit was used 100% of the time to begin another frame and to synchronize the bit stream with circuits to insert or extract a particular channel. This early framing structure became known as D1.

As digital circuits improved, the 193rd bit was timed shared for other functions. D2 framing format, also known as superframe (SF), 12 frames are grouped together. Some of the bits of the twelve frames are still used for synchronization, but others are "robbed" for signal maintenance, error checking and reporting, and communications from one switch network to the next. D1D frame formatting made older D1 systems up-gradable with D2. D3 and D4 also used the twelve frame group. Today the Extended Super Frame (ESF) uses a 24 frame string. T-1 is still used for voice communication, but some, or all, of the 1.54Mbps can be used for direct computer to computer data transfers in networks. Some terms used in testing T-1 services:

BPV- Bipolar Violation, consecutive positive or negative pulses violate the DS-1 standard. Each bit must alternate polarity.

Loss of carrier- 15 consecutive zeros constitutes a loss of carrier, as most circuits must re-synchronize with further bit transmission.

B8ZS- Bipolar with 8 Zero Substitution, a signaling code for some T-1's to prevent two consecutive clear channels from appearing to be a loss of carrier.

BER- Bit Error Rate, expressed as a negative power of ten, that is, 10-8 represents a single error in one billion bits. (11 minutes of T-1 transmission)

QRSS- Quasi-Random Signal Sequence, a simulated T-1 signal that periodically repeats a random sequence of bits.

Digital Milliwatt- An alternating one/zero bit pattern, inserted in every other frame, in three different (out of the eight available) bit positions of a signal voice channel.

NEXT- Near End Cross Talk, close physical proximity of two conductors with different signals may allow coupling part of one signal onto the other conductor, causing errors and interference.

Monitoring cordless phones

These types of phones a very common these days, there are usually a couple just in your neighborhood, or maybe you even own one. Luckily, these are the easiest types of phones to monitor conversations on. The equipment you'll need is a small, 10-channel or more, radio frequency scanner. The cheapest ones are around $100 and are easy to find at Radio Shack, or even some department stores like Wal=Mart, K-Mart, Sears, etc.

First you should know that the FCC put aside ten 46 megahertz, and ten 49 megahertz frequencies for use with cordless phones. Make sure the scanner you get covers these frequency bands. Almost all of them do.

All you have to do is program the ten 46 MHz into your scanner, buy a portable amplified antenna, (Radio Shack cat. no. 15-1607, you'll also need some adapters to take the 1/8 inch plug to BNC, the people at Radio Shack should be able to help you), and walk around your neighborhood. The amplified antenna helps bring in signals that are far away, and helps to increase the quality on closer signals. I have the same set up and was able to bring in conversations two blocks away. Since alot of the cordless phones have the same frequencies you might experience cross-talk (a bunch of people talking, all rolled into one conversation). This should be the only major problem you'll find.

The other ten frequencies are for handset transmissions. They are used if you want to only listen to one party (the person talking on the cordless phone).

If you do experience any other problems you should be able to figure them out by using common sense. Doing this type of stuff is very easy, yet no one knows about it.

HINTS:
A lot of stores use cordless pnones to call in for credit checks, or for maintenance on the computers. They use cordless phones so they can talk and work at the same time. This would be useful to get TRW dial-ups or accounts, passwords to computer networks they might use, or to listen to them call security to remove that kid standing there with scanners and antennas covering him

The ten two-party frequencies are: (in megahertz, MHz)
46.61
46.63
46.67
46.71
46.73
46.77
46.83
46.87
46.93
46.97

The ten one-party frequencies are: (in megahertz, MHz)
49.67
49.77
49.83
49.845
49.86
49.875
49.89
49.93
49.97
49.99

(note: 49.86 is the frequency used in those cheap walkie-talkies)

This article may be a few months late by the time you read it, but it should still be useful in your exploration of the phone company.

Dial up- (414) 682-0879 1200 baud

```
----------------------------------------------------------------------
p>?
p>

CO49 1993 SEP  7 TUE  8 25 18   Rev. 8.58 Program Block Free  19
Unit Number: 1                          Scan Interval: 0 /  1
Attached LCU's: 3
Comm Faults on LCU's: 3
Disabled Vars: 1
History Accumulations: 1,  2,  3,  4,  5,  6

R> THIS IS WISCONSIN BELL MANITOWOC C.O.   NCO49 (414-682-0879)
CURRENT DATE =   9 ,    7 ,    1993     TIME =   825
LAST ALARM #     6, DATE = 9.05 , & TIME =   123
TYPE:     ALARMS    TO CHECK CURRENT ALARMS AND CONDITIONS
          ALARMDIS  TO CHECK FOR DISABLED ALARMS
          LCUMENU   TO SEE LCU COMMANDS
          DEFINE    TO SEE SYSTEM DEFINITIONS

******************** NOTE *********************
          AH2  RENTAL SPACE
          AH3  POWER ROOM
          IS CONTROLLED ON LCU # 2
NOTE - Active chiller selection can now be made thru output #4 (CHLSEL
CT)
-ON selects roof mounted chiller
+ON selects chiller in penthouse

R>p i all
----------------------------------------------------------------------
```

It will show a bunch of information about chillers, heaters,alarms and stuff. It pretty much helps you out. At the R> prompt, P DR 4, or any other number will show the status of drums (some chiller part). Sometimes at the R> prompt, typing &g, will get you these cool history reports. Explore as you wish. If you have any problems or hints about this send them to the Cyber 'Zine staff.

More Phone Numbers-(From the Black Pages)

Easy Link computer system..(Western Union)	1-800-325-4112
RCA...(type LOGIN for id request)	1-800-526-3714
Citibank..(NY,NY)..6 character password	1-800-223-3312
Export/Import Bank	1-800-424-5201
Bank of America	1-800-222-0555
Highland Park Bank	1-312-432-1817
Nanvet National Bank	1-914-623-0402
American Express.(mainframe)	1-800-228-1111
COSMOS.New York)	1-212-370-4304*
COCIS.(mainframe)	1-303-447-2540

* = **may** have the modem turned off(true sellouts)

For the next couple of issues of The Black Book, we will be discussing various types of espionage, surveillance, counter-surveillance, and mission techniques that will help you survive in this world.

First, here are some tips on nighttime operations:

- Since you can't see as well at night, you'll rely more on your ears. Stop and listen often. Try opening your mouth slightly, this will sharpen your hearing. Also remember that noises carry farther at night so be extra quiet.

- If crickets stop chirping, it usually means someone is near them. Remember that when you listen for night sounds.

- If you must whisper, exhale most of your breath first. This will eliminate the "hissing" noise you often hear when people whisper

- When climbing wooden stairs keep your feet near the sides of the steps where they meet the wall. Steps are less creaky at the sides than at the center

- If it's so dark you're afraid you might trip over something, try this walking technique:
    1. Stand with your left foot ahead, your right foot back. Keep your weight on your right foot.
    2. Slide your left foot ahead of you, feeling for obstacles and other objects with your toes.
    3. If the way is clear, shift your weight to your left foot and and move your right foot ahead just behind your left.
    4. Then rest your weight on your right foot again and repeat the process.

The seven Regional Bell Operating Companies (RBOC's), or if your a hacker/phreak the Regional Bell Monopolizing Companies, or the Baby Bells if you don't understand this.

- Ameritech
- Nynex
- BELLSouth
- Bell Atlantic
- USWest
- Southwestern Bell
- Pacific Telesis

These resulted in the 1984 court ordered break-up of Ma Bell (AT&T)
FACT- In 1976 the FCC, in one of their smartest decisions they have ever made, ruled that subscribers could legally own and hook-up their own phones, and phone lines. Basically, this meant that you could buy and hook up your phone yourself, with out having a crazy, drunk, (trust us) Bell worker do it.

The People's Enemy

Wisconsin Bell

AN AMERITECH [redacted] MONOPOLY

Ameritech maintenance systems
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

The following is a list a systems that will be impacted by the SANS program.

SANS is Survey and Assure Network Services, this system will function in the surveillance and assurance required by businesses. It will mechanize and automate surveillance and assurance processes, and continuously check the loop interoffice and switching networks. This system will check for abnormal operations in the loop or switch network, and activate the nessesary procedures to correct the problem in real time. During its monitoring and analysis of the network, SANS can check maintenance messages- including alarms, performance data, and traffic flow data. Once a error is found, SANS determines its source and severity, and provides analyzed trouble indications to the Work Force Administration (WFA). In addition SANS is able to shut down, turn up and reinitialize network elements, cut off local alarm indications, reroute traffic, and control other systems needed to repair the network.

These systems were in the SANS transition plan and are now operational.

1. Ameritech Service Management Systems (ASMS)

ASMS is a software application that allows customers to appear to access the SANS operational support systems. This will allow the customer to track maintenance troubles in their network and control the traffic over their network.

2. Centralized Automatic Reporting On Trunks (CAROT)

CAROT provides demand and scheduled testing of analog trunks and some switched special service circuits.

3. Central Office Equipment Reports (COER)

Provides traffic data measurements using EADAS input Will use NDCOS (Network Data Collection Operating System) data in 1993.

4. Computer System for Mainframe Operations (COSMOS)

A real time computer designed as a wire center administration system for subscriber services. It is responsible for assignment and inventory control of central office facilities. SWITCH will replace COSMOS.

5. Integrated Network Planning System (INPLANS)

INPLANS is a planning application that provides the capabilities to develop integrated plans, plan custom networks, and plan for the rapid deployment of new technologies, architectures, and services, and to track traffic sensitive networks.

6. Network Services Data Base (NSDB)

NSDB is the common data base for circuit information; C1 inventory in the Trunk Integrated Keeping System (TIRKS).

7. Service Management System (SMS)

Provides monitoring and updating of the Common Channel Signaling (CCS) network.

8. SWITCH

The new nodal inventory and assignment components for integrated provisioning, assigns both line and trunk switch ports. It replaces COSMOS and TIRKS/Generic TAS systems while adding enhanced functionality.

9. Trunk Integrated Record Keeping System (TIRKS)

TIRKS provides for the creation and maintenance of equipment inventory and assignment records, and pending equipment orders. It also provides for the creation and maintenance of central office switching equipment assignment records including trunk relay, traffic measuring, and test access. The interface to TIRKS for the SANS system is through NSDB.
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

The Budget Hacker's Tools

Here's what you'll need:

1. Acoustic Coupler, a neet little device that straps onto the ear and mouth piece of a phone. These are used when no modular jacks are around. Example payphones and hotel/motel phones. Available from Computer Products Plus, 16351 Gothard St., Huntington Beach, CA,92647 or call 1-800-274-4277. They are around $140.

2. Modem, external, battery powered ones work the best because they don't use line voltage. You don't need any thing fancy, but one with weird baud rate options helps because some computers think the only security they need is a strange baud rate (600, 1100 baud).

3. Laptop, all hacking done these days is from remote locations, and payphones. Hacking from your house will get you caught faster than anything. Nothing fancy is needed, but make sure you get extra batterys

4. NBC hat, or any other large corporations. The ultimate social engineering prop. If some one asks what your doing, say your sending stories, or business info over the phone lines. It will usually give you a few extra minutes if your at a payphone in a building that's closing up, or removing nosey Rent-A-Cops.

5. Jolt cola, the soft drink of elite hackers. Good for all nighters at a payphone. Goes well with the cheap, $.25 junk food (goop)

MERRY CHRISTMAS EVERYONE!

In the new year the black book will go through many changes. Some of the changes include a new name, new format, and a reader's input page. Due to the major loss of cash the new informational pamphlet will be $1.50 newsstand and $1.00 if you subscribe. The cost of a subscription is $12.00/year and 12 stamps (any way you can get the stamps will be fine with us).

Black book back issues

#1 payphone crap, opening warded locks, hack stamps $1.50
#2 lineman's handsets,fire bottle, phone numbers $1.50
#3 window foil, terminal boxes, frequencies, JJ patch $1.50
(please include stamps if you want them mailed)

NOTE

The JJ Rent-A-Cop patches are free if you would like one just ask. Also, we are looking for people on our staff. If you can type, Hack, or just want something to do; Join us, you make no money, but you can bet you will have some fun.

We will print an article in the next issue
on how to contact us.