Cybertek

Issue #16

Ticom's Zine

"How-To" Info for T... ...ological Enthusiasts

In this issue:

- Telecommunications Info,
- Cable Modems, and More....

Cybertek Issue #16

Table of Contents:

Cybertek

Published by: OCL/Magnitude
P.O. Box 64
Brewster, NY 10509

Publishing Schedule: Quarterly (We at least try to.)

Subscriptions:
Domestic - $15/year Canadian - $25/year (US)
Overseas - $30/year (US) Corporate - $80/year

Trades of similar periodicals, interesting (and functional) electronic equipment, office supplies, envelopes, and 32 or 55 cent stamps accepted in lieu of monetary payment.

Telephony Information Update FAQ

by Black IC/IIRG

Table of Contents

Initially this release was not meant as an end all, if nothing else it was designed to promote questions and get those in the Connecticut scene (and hopefully other states seeing as this information is not segregated to Connecticut) to start thinking about telephony and what the future holds. As time went on and revisions (releases) were done it became a pet project for me to slowly add to it and watch it grow. There can never be an ending to this release. It will simply evolve over time and hopefully help those new to the community with getting a "jump start" on whats going on around us.

This FAQ is a compilation for that purpose.

Seeing as most of this information pertains to Bellcore, AT&T (Lucent) and the major (unknown) industrialists in our telephony dealings, this write up is very much as important to Connecticut and SNET clients as it is to the other states. We have included information about what is going on in our state as well as in other states, mainly PACBELL areas. Why? Because phreaking is moving to a whole new level, one that will change everything we know about boxes, secure dialing, porto hacking, and other esoteric actions.

Why are Red Boxes becoming obsolete?

The coins are registered upon entry by an electronic coin validation device. It actually checks the weight of the coin to a known standard and adds it to the deposited coin list at the CO. Everyone knows there is a magnet to pick up slugs and shut down the phone of course but new phones and existing system phones are being converted as we speak to monitored system phones. Actually the payphone itself is monitored for jams, cut handsets, cut wires, etc. Any problems are reported to a data station in the Meriden Operations Center and a trouble ticket is issued. All this is done with the help of an Intel Chip. Now knowing the speed of the Bell Repairman I wouldn't run as soon as something happens but be careful out there.

Right now their are two phones on the market in the United States that have this capability, the first being:

The MARS-2. It is designed by the technology devision of MARS (M&M Mars Candy) and is in use in Connecticut, soon to be spreading to other states, namely Bell Atlantic areas.

MARS ELECTRONICS INTERNATIONAL
1301 Wilson Drive
West Chester, PA
(610) 430-2500

The second phone is the Nortel Millenium:

It seems that Pacific Bell (PACBELL) and their sister company Telesis in Nevada are in the process of upgrading their pauphones also. The new payphones they will be upgrading to are the Nortel Millenium made by Nortel. These phones will be replacing the ACTS phones they use now. Just as the MARS2 are replacing them in Connecticut. Nevada has just started installing them and Pacific Bell will follow afterwards. Our sister to the North (Canada) has been dealing with the Nortel Millenium for awhile now. The Millenium offers the same features as the MARS2 but also contain the following added features.

1) Phones will be installed with a touch screen video display.
2) Phones will have a calling/credit card slot plus the change slot.
3) Calling cards will have a running credit transferable to a new card when needed.

Where is SNET at in the pay phone series and COCOTs?

- ACTS payphones are going to be obsolete.
- MARS the successor of ACTS is moved into its second generation the MARS2.

What this means is that the payphones are going "smart".

They are going to contain a microprocessor and battery backup. This processor will monitor the phone separate of the CO. If anything is vandalized or a hardware malfunction the payphone will immediately notify the CO for shut down and repair. They will also be usable on POTS lines. This means the Red Box will be obsolete. Done deal. It also means that with the SNET going into COCOTS they can be installed in your house. Now how does SNET stand to gain from COCOTS? Now SNET is not the only company getting into COCOTs. Its only natural that the telcos choose this route.

1) They sell the phone (profit)
2) They sell use of the line (profit)
3) They get payed for maintenance (profit)

They are also planning installing for battery backup. Smart batteries. Made by Duracell and they have the ability to recharge themselves off the black and yellow phone lines connected to a 6 or 12 volt generator (transformer). This would keep all the wires self contained and secure.

What is the laptop the repairmen use?

The SNET lineman are using a RANDOM COMPANION laptop at the moment. It's a DOS based system that they use to call the mainframe via an 800 number in New Haven. There are about six things you need to do to access the system from a

remote sight. The toughest being the ACCESS card they use. Its like a credit card that is timed with the computer in NH every minute it changes its number and you have to have the number to get into the system. It is by far the tightest system I have ever seen in terms of hacking but if you can get in you have access to tons of company documents including line records and billing info.

What can we expect for baudrates from our POTS lines?

"SNET will guarantee the transmission of data at a speed of 9600bps or less."

Every telco will tell you that they only guarantee a certain amount of BPS on a POTS line. NYNEX only allows 4800bps for their phone lines so I guess we're kind of lucky. Fact is you can get good connects, its long distance that is a problem and until the Local Carriers upgrade their analog lines to digital, we have to deal with the annoying problems.

Its not uncommon for a telco service representative to try and get you to commit to a balnced line, a line that will handle higher baudrate. What they dont tell you is that aside from the outrageous leasing prices and installation charges you have to purchase the rest of the line if its not readily available in your area. I think not.

In the sidebar is a basic run down of how the POTS line deals with the data and what you can expect. Also enclosed is the SNET statement regarding said lines.

In a nutshell if the line tester finds that your line meets the standards specified above you will have to pay for a balanced line if you want to TX at greater than 9600bps. I think the starting rate for a balanced line is around $150.00 depending on what you want. In addition since SNET owns the cable plant and leases space (pairs) to the other dialtone providers you cant go anywhere else.

What are SNET and other telephone companies doing for Multi-Media?

SNET is working in cojunction with AT&T, TCI Cable, Scientific Atlanta, Hewlett Packard, and SEGA games on a limited level (SEGA Channel) for a future in VOD (Video On Demand) and to bring about a joint telephony/cable business (VDT at a TV near you). They are also looking to have fiber-optics implemented fully in the next 5-10 years.

MINIMUM TX STANDARDS

Loop Current (ma) >20
Loss (db) <8
Attenuation Distortion (slope) <-3.0/+12.0
Noise (dbrnc) <30
Longitudinal Balance (db) >50
Noise to Ground (power influence) <90

Attenuation distortion or slope is the difference between the loss measured at the low and high frequencies, relative to the measurement at 1004hz, usually expressed at a range in the form of two numbers as stated above.

SNET designs its POTS lines for analog voice transmission. If our POTS lines meet the MINIMUM TX STANDARDS, SNET will guarantee the TX of data up to a speed of 9600bps. If there is a problem, SNET will perform transmission paramater testing, and if the line fails to meet the minimum standards, SNET will support the redesign of the line so it meets the standards specified above. If the problem lies with the CPE (modem or fax) there is nothing more that SNET can do. At this point the tech should refer the customer to his/her CPE supplier.

Here is how some of the work load is being dealt with.

Hewlett Packard (Main operating system of SNET) and Scientific Atlanta (ATM Broadband Integrated Gateway OC-3C which provides the gateway between a SONET network carrying ATM and the broadband cable network. One of its purposes is to remove the jitters introduced by ATM switching and transport) are doing a joint project in effort to better increase service over the analog system, create a stable enviroment into a multi-media operation and provider. This is done through various equiptment (as listed above) designed by Scientific Atlanta (SA) and software/computers by Hewlett Packard (HP)

to assist in this transition.

AT&T setting up and testing the LD lines and allowing SNET use of those and local equiptment. This is part of the I-SNET (Internet Provider) program.

TCI Cable and SEGA Channel working with SNET to increase multi-media options for there respected customers.

Broadcast video arrives from VIP (Video Info Providers) on coax to BBOT (Broadband Optical Transport Bay). Can be split four ways to support up to four Fiber nodes.

Video information is analog broadcast and digital video information.

- Analog broadcast is local TV sation AM-VSB Format.
- Digital broadcast is VOD,EPPV... i.e. Showtime, Disney, CNN, etc.
- IMTV (Interactive Multi-media TV) 2-Way interaction with VIU. i.e. Home Shoppers Guide, Games (SEGA Channel), etc.

PairGain HiGain Line Unit is one of the many pieces of hardware that they are using for all of this.

This unit is the Central Office side of a repeater-less T1 transmission system.

When this unit (HLU-231) works in cojuntion with a HiGain Remote system (HRU-412) the system provides 1.544Mbps transmission on two unconditioned copper pairs over the full Carrier Serving Area (CSA) range.

The CSA includes loops up to 12000 feet of AWG 24 or 9000 feet of AWG 26 wire, including bridge taps. The HDSL (High-bit-rate Digital Subscriber Line) transmission technology as recommended by Bellcore.

This system provides a cost effective way to deloy an easy method for delivering T1 High Capacity Digital Service

(HCDS) over mettalic pairs. The fiber like quality service is deployed over two unconditioned, non-loaded copper pairs. Conventional in-line T1 repeaters are not required. Cable pair conditioning, pair separation and bridge tap removal, are not required.

Is SNET in the security business?

Seems SNET is getting into the Security Monitoring Systems game too.

Right now for (what I believe is BETA testing) SNET Employees, they are offering deals to get or switch to the SNET Security Systems. Right up ADT's alley.

A proprietary interactive Commander 2000 wireless alarm system expandable up to 17 zones. Not to mention the whole nine

WHAT ARE THE FREQUENCIES OF THE MULTI-MEDIA PROGRAM?

Multi-Media/I-SNET/Telephony Bandwidth Allocation using AT&T equiptment:

5-15 MHz - Not used
15.4-17.8 - IPPV/Analog set top box
17.8-21.0 - Digital set-top signaling
21.0-21.4 - Upstream status monitor
21.5-25.0 - Not used (reserved for MM or telephony)
25.0-40.0 - Upstream telephony
40.0-50.0 - Upstream/downstream transition
50.7 - Sweep pilot tone
54-88 - Analog video
72-76 - Downstream digital signaling
88-108 - Analog video/SEGA/DMX
108-120 - Digital set-top signaling/analog video/SEGA/DMX
439.25 - MM video carrier for CCOR
120-547 - Analog video
547-551 - ALC and status monitor (CH.78)
551-700 - Digital video
700-750 - Downstream telephony

yards of window sensors, etc.

Who is going to be a player in the Local Exchange Carrier Business?

When a telecommunication company wishes to provide local exchange service, they must first apply to the Department of Public Utility (DPUC) for a Certificate of Public Convenience and Necessity (CPCN) or a request of expansion of an existing CPCN. In this application, the company must demonstrate both the financial resource and the technical ability to provide the services defined in the application. Additionally, the application will include the areas of the state where they will provide service and the general method of providing the service (i.e. resale of bundled services or facility based provider). The application will follow the normal DPUC regulatory process including testimony and hearings. If the application is approved, the company is granted a CPCN for these services and becomes a Certified Local Exchange Carrier (CLEC).

As of right now, nine companies have applied for CLEC status, seven have been approved, one is pending and one has withdrawn. The approved companies include; TCG, AT&T, MCI, MFS, Brooks Fiber, LDDS Worldcom, and Cable & Wireless. Cablevision Lightpath is pending and Sprint Telecommunications Venture (STV) has withdrawn their request.

We know MCI and AT&T are in cohoots, with the merger of NYNEX and Bell Atlantic we can only imagine how things are going to develop.

Is SNET playing fair?

The following web site provides a list of all Connecticut internet providers as a service to their customers.

http://www.fcc.com/ctisp.htm (Computerized Horizons).

Seems this site has removed SNET from the list and labeled SNET as a "Hostile Competitor". They claim SNET can't actively attack competitors and get free advertisement at the same

time, makes unfair and misleading statements about its competitors, which goes against everything that has been done regarding ISP's.

They will at their discretion determine who is a "Hostile Competitor". They define that as a company that makes unfair attacks at other Connecticut ISP's... and to be fair they will list those said companies. Right now SNET is the only one on the list.

You might want to check out the Web if you live in another state to try and find out what your telephone company is doing in regards to the internet and its services. You might be suprised.

5ESS-2000 DCS Vulnerability

The 5ESS-2000 DCS is strictly the cellular switch. DCS (Digital Cellular Switch). It seems SNET as well as the other telcos that use this switch are having having major troubles keeping this baby from going "Critical Alarm" at the CO.

This sytem is used soley for the cellular activities and not any combination of cellular and line type end office. A few are inappropriately set up to handle AMA (Automatic Message Accounting) billing. As a result there have been errors that have shut the system down and sounded the alarm at the respected CO.

To clear this problem they are taking the following steps at the appropriate DCS terminal:

5ESS-2000 Switch DCS UNIX terminal:

input: "cd /database/amafiles"
input: "/no5text/prc/amnullcf > config.oc"
input: "/no5text/prc/amnullcf > config.ic"
input: "cd /database/amabfiles"
input: "/no5text/prc/amnullcf > config.oc"
input: "/no5text/prcamnullcf > config.ic"

This will alleviate the problem for that station but not the others. Make a note of some of the directories for further use cause this is where you will find the billing information provided you dont hit up a system that has had this re-done.

The billing is done on the ESS. ESS5 has an awesome billing, regulating section. They had designed the ESS-2000 the cellular digital switch and unfortunately they found they couldn't manage the billing well on their (read: securely) so they have it dealt with on the ESS5 switch as it should be. If by some chance you gain access to a ESS-2000 you can check to see if it is secured or not. If it isn't you will be able to get billing info from the 2000. Just make sure you change directories to /database/amabfiles. Automatic Message Accounting Billing Files is the place to be. The same goes for standard ESS5, you'll want to check out that directory their.

AT&T Comment on the Telco Bill

AT&T comments on House passage of the Telecommunications Bill

> WASHINGTON -- AT&T issued the following statement this afternoon following passage of H.R. 1555 in the House by a vote of 305 to 117. The House vote was no surprise but is nonetheless very disappointing. The House had an opportunity to take a bold step toward reform but retreated. It backed away from a Commerce Committee-passed bill that would have advanced competition by forcing the Bell companies to face real competition.
>
> Although the bill establishes the theoretical conditions for opening the local telephone exchange, it frees the Regional
> Bell companies to extend their monopolies into the competitive long distance business before they face broad local service competition from a rival company with its own network facilities.
>
> But this unbalanced legislation isn't law yet. Along with others, AT&T will continue to work to achieve a balanced

result when the legislation is considered by a House-Senate conference committee later this year. In conference, we will urge members to strive for true reform and ensure competition through all segments of the industry. The fact that a number of the objectionable provisions of the House bill remain contentious, as evidenced by today's key vote totals, provides encouragement that a better

ᛗ

Another Perspective On the Cable-Modem Problem

by "Unattributed"

The more people start info-groping about the Highway-1 Cable Modem internet service offering, the better. There seems to be a tradition of technological one-upmanship between hackers and the cable industry, and this is obviously going to open a whole new playground for that sort of thing. Here's what I currently know, conjecture, and ask, and I'm not even a subscriber.

The cable modems are manufactured by LanCity, now owned by Bay Networks. There are several web pages at the still-extant LanCity site that are surprisingly informative about the modems. I currently have no plans for getting the service myself [and it's not yet available where I live either], but the web info and discussions with a couple of early adopters have gotten me curious about the things too. Other people have already noticed the ease with which their Macs and Windows boxes can see their "network neighborhood", which illustrates the potential for a real security nightmare.

I went to the Networks Expo show a couple of weeks ago and finally got to physically examine one of the modems. Interestingly, the manual for it was nowhere to be found in the booth. I was informed that the weird heatsink design is not so much for dissipation as to prevent people from putting things on top of

the modem. I chatted for quite a while with someone from Highway-1 who seemed relatively clueful and not *too* suspicious about why I was asking about in-depth technical stuff. I raised a lot of my questions with him, and he freely acknowledged that many of their engineers are relatively new to this here Internet Thang, but they're at least aware of where the problem areas are. There are many reasons they retain ownership of the cable modem – they *must* be able to control all aspects of its operation from their headend, or customers would be able to waltz off and obtain much greater levels of service than they ostensibly paid for. As we talked, I posed several "what if" scenarios as questions, and at one point he said something like "we are addressing many of these concerns, but sure, if some propeller-head comes along and really tries to break it, he probably will." Hmmph. Where'd I put my fucking TITANIUM BEANIE...

To defend against the point I raised about customers seeing each others' machines and being able to print porn on each others' printers, he said that the upcoming new LanCity firmware release will include various kinds of filtering and that they intend to use it. While most customers don't notice or care if certain IP traffic to or from them is blocked, there will always be the vocal few [like myself, probably] who howl about it and insist that they have a completely "raw" connection to the internet. Many providers refuse to provide any customer-specific filtering because of this management headache, and those that try to are notoriously inept at it anyway, so we'll see...

I could not get much information about how the modems self-configure when they come up. My best guess based on what the guy said is that they start searching some predefined range up among the higher frequencies for "carrier channels", and information about the corresponding backchannel frequency is somehow embedded therein. The backchannels are down at 30-something MHz, which is why the high-pass "noise filter" must be removed at the pole. It is also unlikely that another brand of cable modem would work with this system, since the exact protocol that LanCity uses is one of several competing methods that exist. The standardization battle over cable-plant data transmission is apparently still going on.

Someone else may already know much more about the specific modulation and framing schemes. One interesting thing the guy at the show mentioned was that while spectrum analysis of a standard 6 MHz TV channel would show two peaks where the sound and video carriers live, the display of a data channel would b a "solid block all the way across" stopping just short of the band edges. It is possible that something would turn up by tuning through the cable channel range, perhaps using an old analog TV and a UHF block converter and carefully watching and listening.

One thing that struck me as somewhat sleazy is the fact that these modems are fully capable of doing 10 megabits in BOTH directions, and HW-1 configures them to deliberately throttle back to the advertised speeds. I guess this is their way of "capacity planning" or something. There was a strong hint that higher speeds, and routing to non-DHCPized blocks of IP address space, will be sold as more expensive higher-end services starting later this year.

As someone else mentioned, hosting an entire house full of computers still isn't hard if the single dynamic IP address is one side of a NAT or proxy server. I was told that the standard residential service will indeed only work with a single known MAC address, such that if someone just dropped in their own modem and tried to come up on the net, the DHCP server wouldn't respond and possibly the mechanism that assigns transmit and receive frequencies wouldn't either. This is one reason they either sell you the net card or need the MAC address from a [supported] one you already own, and specifically configure for it. It also confirms some other peoples' experiences. So far it sounds like they've rigged things so that in theory one needs the following things to be able to use the service:

- a recognized MAC address
- the backchannel high-pass filter removed at the drop
- the right model of LanCity modem
- Possibly some magic configuration in said modem [auth keys? MAC addrs?]

Since the box behaves like a bridge, one presumably cannot run

a promiscuous packet sniffer on the customer side and see the neighborhood traffic. I guess this would include HW-1's management traffic as well. I suspect that being able to observe the management traffic would blow the whole game wide open. Someone able to freely reconfigure their own modem could probably come up as any in-subnet IP address they wanted, from any MAC, at any speed, on any frequency pair, completely bypass any accounting, and play all sorts of nasty games. Ten-bit subnets implies a potential for 1022 devices per neighborhood, which would give a large range to select from.

The logical block diagram of the modem would probably have at least the modem and bridging components as separate subunits, and may quite possibly exist inside as separate physical chips. Some trace between two such chips may carry the raw data from the cable plant in a convenient Ethernet-framed format, which would be the obvious interesting tap-off point for monitoring. Someone should try this. HW-1 would undoubtedly go nonlinear if a customer takes the modem apart to poke at the innards and the box may even implement some kind of tamper switch, but then again thousands of cable converters have been torn open for a looksee in the past...

I investigated some small chunks of their network space, and what I observe so far does *NOT* give me a particularly warm fuzzy feeling about how they are handling security issues after all. I dumped the "ne.highway1.com" DNS zone, excerpts from which are included below, and the first thing that disturbs me is that they're mapping IP addresses to the real-life names of customers or at least strong hints thereto. The second thing I noticed is a bunch of CNAME entries that are obviously MAC addresses -- quite likely those that their DHCP server will recognize. They've just given away a piece of information I might be able to use in conjunction with a changeable-MAC-address ethernet card to pretend to be a legitimate customer. Of course they are only using one brand of NIC anyway and probably bulk-ordered them in big batches, so the search space for valid MAC addresses is probably small to begin with. Also, each modem may be hard-configured at installation time to only work with one MAC on its ethernet sid. Still, must they be so obvious about it? And while in the "obvious" department, the

names of devices within their own infrastructure hint strongly at where they are and what they do, beginning with 24.128.1.60.

But most disturbing of all is what I observed upon firing in a couple of generic sysinfo-ish SNMP queries. A surprising number of devices respond to queries using community names "public" *or* "private". A fragment of the somewhat raw-format scan output is included below. To convince myself that these really were the configured community names I sent in some probes with some random name, and got no response -- so it appears that they really are using vanilla SNMP v1 with factory default names on the LIVE NETWORK. Not only were several of the modems reachable with such probes, so were their *backbone cisco routers*. *This* is the "secure SNMP" network management" touted on the LanCity web page?! Lacking a handy build of the CMU SNMP toolkit, I didn't try actually setting any variables or walking the entire MIB, but I would be interested in seeing any results from other folks.

There are several other interesting points about the active modems. They only appear to support UDP protocol and have no TCP stack, handing back "ICMP protocol 6 unreachable" for any TCP probes. Their addresses seem to be semi-randomly sprinkled around amongst customer IP addresses, but never have DNS entries. This [along with hints on the LC web pages] implies that the modems themselves DHCP for their own addresses but don't get the dynamic DNS mapping.. How, then, is the HW-1 management staff able to map the active modem addresses to specific customers? This would also imply that each active customer effectively occupies *two* IP addresses.

The SNMP string "LCP" maps to the "single user modem" product. The web pages also describe the LCb and LCn products, the latter of which is the centralized "provisioning server" -- based on Microsoft Access?!?!? Obviously if that single box falls, the entire network is at risk. There's a claim in there that configuration data is DES-encrypted in flight to the modem, which sounds like the vault door on the front of the house with the flapping SNMP screen door on the back. I'm not sure why we see the string "Andover", but it almost makes sense given that LanCity's offices are located there. This is relatively

nearby, and I think it's high time for a dumpster dive.

DNS stuff

```
ne.highway1.com   86400 IN NS
        chnms01.highway1.com
ne.highway1.com   86400 IN NS
        chnms02.highway1.com

jajones.ne.highway1.com     86400 IN A      24.128.53.3
johnk.ne.highway1.com       86400 IN A
        24.128.38.248
bobson.ne.highway1.com      86400 IN A
        24.128.63.214
anntk.ne.highway1.com       86400 IN A
        24.128.45.182

dedham_3.ne.highway1.com 86400 IN A      24.128.8.13
watertown_9.ne.highway1.com         86400 IN A
        24.128.60.32
wilmington_13.ne.highway1.com       86400 IN A
        24.128.44.47
wilmington_14.ne.highway1.com       86400 IN A
        24.128.44.48

0000ca032a28.ne.highway1.com        86400 IN CNAME
        winchester_3.ne.highway1.com
0000ca0306cc.ne.highway1.com        86400 IN CNAME
        natick_7.ne.highway1.com
0000ca0306b2.ne.highway1.com        86400 IN CNAME
        wellesley_17.ne.highway1.com
```

SNMP queries

```
(UNKNOWN) [24.128.45.195] 161 (?) open
private
LCP SUWGB
Administrator0
LC-Bridge0
Andover0
```

(UNKNOWN) [24.128.45.196] 161 (?) open

ayvazian.ne.highway1.com [24.128.45.197] 161 (?) open

(UNKNOWN) [24.128.45.198] 161 (?) open
private
LCP SUWGB
Administrator0
LC-Bridge0
Andover0

lawrence-rtr-a.highway1.com [24.128.0.249] 161 (?) open
public
Cisco Internetwork Operating System Software
IOS (tm) 3000 Software (IGS-P-L), Version 11.1(8), RE-LEASE SOFTWARE (fc1)
Copyright (c) 1986-1996 by cisco Systems, Inc.
Compiled Thu 05-Dec-96 13:00 by tamb0
lowell-rtr-a0

Further Personal Experiences

Recently I swung by the back of LANCity's building again and in contrast to earlier attempts, was able to indulge in a classic info-gathering dumpster dive. The most surreal part of it all had to be the site security guard that wandered by a couple of times and seemed somewhat amused by my presence and made NO effort to discourage me or tell me to leave. It was broad daylight, I had parked right next to the dumpster with the car still running, and was being careful to not make a mess, so he perceived nothing shady going on but it was still way WEIRD to stand there in a half inch of chilly water surrounded by bags and boxes and chat amiably with this uniformed gent through the open hatch.

I didn't find any cool hardware, but I did dig out all kinds of entertaining sales orders, org charts, the timeline for their next product development into October 1997 or so, and a bunch of other random stuff including extensive corporate asset and customer lists. There were only about 6 findable copied pages of what I *really* wanted, that being the manual with all the

SNMP variables, but what I recovered provides a couple of hints at what can be read or controlled and confirms the fact that an operations manual with that level of detail *does* exist.

It appears that the current problems are not really LANCity's fault, and that they do try to provide the security features that we would expect. But the providers that buy and install this stuff as a turnkey system, without making the necessary configuration changes, just throw themselves wide open to various abuses. I expect that someday they'll get a few hard knocks and finally buy a clue, but it will likely be reactive instead of proactive.

In other news, it is now confirmed that the Highway-1 backbone routers are configured to pass directed IP broadcast, which in combination with SNMP arp and routing info allows for very fast network topology probing from the outside. Their web and shell servers appear to be based on largely out-of-the-box Solaris. But most notable of all, the default SNMP write community *does* allow changes to be made to the modems and other equipment. That's pretty serious -- they are really bending over and begging for it...

More recently it appears that someone over there has finally clued in, and fewer devices respond to SNMP community "private". But "public" still seems as ubiquitous as ever, so who knows. Again, if just one enterprising customer manages to sniff the cable-plant side of the modem for a while, it's all over. It is likely that even if the write-community has changed, it is used in *all* the devices from customer modems all the way up to the headend controllers.

Oddly enough, Continental Cablevision has apparently changed its name to Media 1, offering a "single source for cable TV, high-speed Internet access, and videoconferencing". Less than a week after the "big announcement" I was out biking, and a van painted up with the new Media 1 logo went by me, so they must have been planning this for quite a while.

BLACK IC/IIRG PRESENTS MERLIN PLUS COMMUNICATIONS SYSTEM [3] MERLIN MAIL SYSTEM (VMS)

There are a number of Voice Mail Systems (VMS) available to the general public and private sector. These systems serve a purpose of being an automated answering service and toll-free communication via messages. Of the ones out there none seems more fit for the private sector than the AT&T MERLIN Voice Mail System.

Because the MERLIN is comprised of several different components and designed to be upgraded and modified to work in a number of environments, it's very appropriate for businesses and specifically law enforcement usage. It can be incorporated easily with the E911 system or a simple connection to a corporate office. Whatever the application it is quite an amazing system.

This overview will cover the basics of the MERLIN systems specifically the MERLIN Plus and its hardware, points of entry that you should look for, and theory of gaining entry to one of these systems.

MERLIN CONTROL SYSTEM OVERVIEW

The MERLIN Control System is the bread and butter of this puppy. It contains the software so that you can customize your system to your needs. Anything that is added or taken away is the clients business and this system will handle it. Without the Control system, no other add-ons will work.

The basic parts are the cartridges which depending on the type allow you to do several things from custom features, audio options (music) and power backup for messages and announcements. Four POTS lines going in and voice terminal jacks going out to the various add-ons like the mail system.

MERLIN ATTENDANT OVERVIEW

The MERLIN Attendant offers a wide range of security and customer relations for the owners. The main purpose is to answer incoming calls with a pre-recorded message just like an answering machine and then direct the caller to the appropriate extension in the MERLIN Plus Communications System. This will reduce the workload of the receptionist, insure that incoming calls are answered during peak hours and that they are answered after business hours or when the office is closed like on holidays. This system was designed for these purposes and you can see how they would be perfect for a major corporation or law enforcement agency aspect (E911).

Some of the other features that the MERLIN offers are security, remote programmability and multiple announcements. The security aspect offers a security code that the callers MUST enter before changing any programmable feature to protect recorded announcements and other programmable parts from being changed by any unauthorized personnel. This code is defaulted anytime the system is installed or revamped. I will get into the different defaults and what you can expect later on in the article. The remote programmable aspect allows callers to remotely change announcements if they have access and certainly different parts of their account like passwords. The multiple announcement feature allows different announcements based on time of day or type of call (i.e. Emergency or General). The system will also keep track of business hours and days of operation by an internal clock thus allowing appropriate messages based on that. There is a battery backup in the system in the event there is a power failure the cutomer service aspect is not affected.

The basic look of the Attendant Component was designed to assist an operator at the station to know what is going on with the system with the minimal amount of training. Consider it an idiot-proof system, and because of that, it's widely popular. The Attendant Component merely has 3 lights on the faceplate. That's it.

The purpose of these lights are as follows:

SWITCH	On (Down)	Off (Up)
1	Announcements Saved During Power Outage.	Announcements Not Saved During Power Outage.
2	Programming Parameters Saved During Power Outage.	Programming Parameters Not Saved During Power Outage.
3	MERLIN Attendant Continues To Answer Calls During Power Outage.	MERLIN Attendant Does Not Answer Calls During Power Outage.
4	NOT USED	NOT USED

1) POWER: Self-explanatory. Either the light is on and thus denoting power is going to the system or its not and thus it not plugged in or has a mechanical failure.

2) BATTERY: The light is off if the battery is not fully charged otherwise it's on. Troubleshooting comes in when both are off or the power is on but the battery light is "BLINKING".

3) TALKING: Whenever the MERLIN Attendant answers a call or is monitoring a call this light will be on.

The MERLIN Attendant rear panel is again a design of simplicity.

The purpose of these connectors are as follows:

1) RESET: Used to reset the MERLIN Attendant when there is a need to troubleshoot a problem.

2) SETUP: The SETUP contains four switches that are set to make the Attendant react a certain way to calls. They are on Page 23.

3) 10VAC: Power Connector.

4) SERIAL I/O: Printer Hook-Up and Diagnostic Hook-Up.

5) AUDIO OUT: External Speaker though not used regularly.

6) RESERVED: Another phone line though not used regularly.

7) TO LINE: Connects to the POTS line and modem interface which in turn connects to a module on the MERLIN Plus system control unit.

That's the basics of the MERLIN Attendant Module. It allows or disallows access based on the proper codes. It also will transfer callers if allowed to the right party. If the receptionist is not available after a certain amount of rings this unit will answer the phone and take over. It's not a requirement to have this as a front end. But it will be incorporated at some point in the system either as primary handler of calls or secondary. Remem-

ber that the MERLIN Systems are not one unit per se' they are a bunch of units connecting together to get a certain job done based on the requirements of the application needed.

MERLIN MAIL SYSTEM

The MERLIN Mail System is designed to handle four hours of message storage. Its voice-processing card has two ports that connect to the telephone lines. It's also available in two and four port setups. Once these ports are connected to the telephone modules it will appear as single line sets to the MERLIN system. They also come with an RS-232 serial port to support remote maintenance and allow remote administrative capabilities.

That's the gist of the voice mail aspect of the system. Very simplistic even in its usage. The attendant is considered a small portion of the system that is highly configurable, where as the MERLIN Mail System aspect is equally important in the process of storing messages and allocating mail boxes.

MERLIN Mail System phones are special phones with displays that show you the status of your mail box and if/when a message comes to the box a green light will turn on, thus denoting you have mail.

With all the information shared you can see that this system will react differently depending on how it is set up. You may get a general message or you might get a menu of available commands. Whatever the case, they are all changeable via remote, which brings me to my next topic.

MERLIN MAIL COMMANDS

This is a portion of the Merlin Mail commands list:

*7 Enter Voice Mail
(Extention) followed by a
(Password) followed by a

Do this at point of greeting the rest are prompt issued and can be easily followed.

To create a new mailbox:

Follow commands above and:

Press: 9 to administer MERLIN Mail
Press: 4 for mailbox administration
Press: 4 to create a new mailbox

Enter the extention of the person to be assigned the mailbox
Enter the Class of Service (COS)
Enter the users last name (first 10 letters) using the "Letter Key" followed by a #

Follow the prompts.

*7 at anytime in the mail box will allow you to switch to another extension. Again follow the prompts.

Changing your password, forwarding mail, and transfering your mail are all part of the prompts you can listen to.

Class of Service (COS) is a flag that sets how much time a message has on the mail box and whether it will be supervised or not supervised. The codes for the COS and what they mean are:

Class of Service (COS):

1 = 05 minutes Unsupervised
2 = 10 minutes Unsupervised
3 = 15 minutes Unsupervised
4 = 05 minutes Supervised
5 = 10 minutes Supervised
6 = 15 minutes Supervised
7 = 05 No Transfers/Most Restrictive

Here is the "Letter Key" list that you will need to enter the name of the mailbox and is not given in prompts:

A = 21	N = 62
B = 22	O = 63
C = 23	P = 71
D = 31	Q = 74
E = 32	R = 72
F = 33	S = 73
G = 41	T = 81
H = 42	U = 82
I = 43	V = 83
J = 51	W = 91
K = 52	X = 92
L = 53	Y = 93
M = 61	Z = 94

HACKING THE MERLIN SYSTEMS

Most of you are familiar with Voice Mail Systems and as such probably just want to know the goods about this one. Well the goods are a list of commands and defaults. That wont do you any good though if you don't understand what they mean and most certainly if the defaults have been changed. The way the mail system works is based on in-house extensions, what level that service will be at, and passwords. You can change your password at anytime with out an issue and the system administrator can change yours to, which if you lost yours he would set it at the default. The only way the system administrator can change his own password is if it's done in-house and with the assistance of AT&T. AT&T has an issue with hackers obviously, but they also will adjust to the needs of their clients even in light of a security risk. Thoughtful customer service brings human error.

If you reach a MERLIN system try and get a number of one of the in-house offices. Most lines when installed in an office building are done in groups and in doing so they tend to have consecutive extensions attached to their respected office line. If you get one, add 5 and subtract 5 to that number and you can be sure that you now have 11 extensions to play with. Better yet

call up the office during day hours and grab a few from the operator. If social engineering is not your forte' don't sweat it. Get a buddy who can work people to do that.

The format for a mailbox will be the extension and password, There is a Class of Service (COS) that is involved but it only denotes what kind of access that mail box will have and how much you can do with it. So it's good to bag an extension that wont have any restrictions (not that you could tell). You don't need a system administrators mail box to have no restrictions.

Extensions will follow the format of a 4-digit number. This number can be anything, and you can get that quite easily. The password is in a 4 digit format also, with major corporations that use the MERLIN Systems it wont be that difficult to brute force the account. People think in terms of alpha/numerics and as such you can come up with words like LOVE that will equal 5683 or any other common word (names). Also parts of birthdays, special years, portions of a social security number are valuable and easily acquired. If your brute forcing using numeric information, the first 4 digits of those listed above will likely be a password of a mailbox. Default passwords and extensions are:

Extension: 9997 (System Administrator)
Password: 1234 (System Administrator)

Extension: 9999 (New General Mailbox)
Password: 1234 (New General Mailbox)

Extension: #### (Find an extension as I stated for the company)
Password: 1234 (Default for new boxes, some will be left unchanged)

As I stated earlier in this write-up, major corporations will use this as well as the E911 system. If there is nothing more that I have an issue with, it is fucking with emergency systems. Please if you find one that carries the MERLIN systems. DO NOT HACK IT. Leave it alone. Hacking is a means to an end, not the end of someone's life if you were to mess with an E911 system and delete important information. I'm not big on the

morality play but if you think fucking with emergency systems would be fun, you have a lot of growing up to do. There are plenty of corporations out their that use the MERLIN's for you to have fun with. All that aside, have fun.

GREETINGS AND THANKS

As always greetings and thanks to the following:

Thomas Icom/IIRG/Cybertek, Mercenary/IIRG, Jim/Today is a good day for Banana Fish, The rest of the IIRG and any Self-Reliant Individuals

Next venture for write-ups: Meridian, AT&T Enterprise Systems, Vesoft and the HP3000 Revisted

Anyone interested in getting in touch with me can e-mail me at black_ic@iirg.org or you can telnet to the BBS there, login as bbs with a password of pfte.

Black IC/IIRG - Administrator iirg.org

International Information Retrieval Guild
May Odin Guide Your Way!

The Second Gives You The Other Nine

BOWSIG Bulletin

News from the Boston Wireless Networking Special Interest Group.

Ok folks, The BOWSIG list has risen again... Please communicate all progress and subscription requests to <bowsig-list@radio.guerrilla.net>

Just a quick update:

We've finally got the radio box (yes the one that runs this list) configured to originate and receive connections via AX25.

When you connect to either of these radio's you will be created an account on the radio box, with the username of your callsign. You will then be given a shell on the box. Yes this is an unrestricted shell at the moment and you can telnet or ssh anywhere. Please remember whatever you type is in the clear over the radio waves.

Eventually, those interested will be given access to the machine so once, one ssh's into the box, they may then connect out into the radio network from there by using:

We will be working on configuring IP tunneling in AX25. We also are working on setting up a one-time password scheme (ie: S-key) for a bit more security.

We are also building up a second radio box with a soundcard to utilize the 'softmodem' software for a 9600bps link on 440MHz soon.

That's all to report for now.

Communicating with Cybertek

Cybertek now has some BBSes which have been made available for its subscribers:

Our main BBS is Cybercraft. It's a POTS dial-in system running 14.4K, and it's phone number is 914-878-7285.

We also have two telnetable BBS systems the first is Osuny. Telnet to osuny.com with a username of bbs and no password. The second BBS is PFTE. Telnet to iirg.org with a username of bbs and a password of pfte.

Our web site is also hosted by Osuny, and can be reached via the URL of <http://www.osuny.com/~areff/>.

Should you wish to send us email. We can be reached via <areff@osuny.com>.

IF "CYBERPUNK" IS THE USE OF AVAILABLE OR APPROPRIATED TECHNOLOGY TO OBTAIN, ANALYZE, AND DISSEMINATE INFORMATION RELATING TO SURVIVAL OR PERSONAL FREEDOM, THEN CYBERTEK IS THECYBERPUNK 'ZINE...THE DISCLAIMER "FOR EDUCATIONAL PURPOSES ONLY"...LETS YOU KNOW THIS ISREALLY ABOUT GETTING YOUR FEET WET AND YOUR HANDS DIRTY.
- JEROD PORE, WIRED MAGAZINE

Cut Here

NAME:_____
ADDRESS:_____
CITY:_____
STATE:_____ZIP_____

__ Subscription to Cybertek ($15)
__ Subscription to Cybertek and Modern Survivor ($22)
__ If renewing your sub, check here.

Please enclose check or money order and mail to:

OCL/Magnitude
P.O. Box 64
Brewster, NY 10509

Cyberfak

OCL/Magnitude
P.O. Box 64
Brewster, NY 10509

32