Internet Paging Terminal
Version 2.34

Hark Technologies

January 14, 2013

Copyright

Changes

The material in this document is for information only and is subject to change without notice. While reasonable efforts have been made in the preparation of this document to assure its accuracy, Onix Electronic Systems Inc. assumes no liability resulting from errors or omissions in this document or the use of the information contained herein. Onix Electronic Systems Inc. reserves the right to make changes in the product design without reservation and without notification to its users.

Hark Technologies Software License Agreement

In return for acquiring a license to use the software ("Software") and related documentation, you agree to the following terms and conditions:

1. License. This Agreement grants you, the Licensee, a license to: (a) use the Software on a single computer system or, in the case of a multi-user or networked system which permits access to the Software by more than one user at the same time, at a single working location: and (b) make one copy of the software in machine readable form solely for back-up purposes provided you reproduce Hark Technologies notice and any proprietary legends.

2. Restrictions. You may not distribute copies of the Software to others or electronically transfer the Software from one computer to another over a network. You may not use the Software from multiple locations of a multi-user or network system at any time. The Software contains trade secrets and in order to protect them you may not decompile, reverse engineer, disassemble, or otherwise reduce the Software to a human-perceivable form. YOU MAY NOT MODIFY, ADAPT, TRANSLATE, RENT, LEASE, LOAN, RE-SELL FOR PROFIT, DISTRIBUTE, NETWORK OR CREATE DERIVATIVE WORKS BASED UPON THE SOFTWARE OR ANY PART THEREOF.

3. Ownership of Software. As Licensee, you own the media upon which the software is recorded or fixed, but Onix Electronic Systems retains title and ownership of the Software recorded on the original media and all subsequent copies of the Software, regardless of the form of media in which or on which the original and other copies may exist. This license is not a sale of the Software or any copy.

4. Confidentiality. You agree to maintain the Software in confidence and to not disclose the Software to any third party without the express written consent of Onix Electronic Systems. You further agree to take all reasonable precautions to preclude access of unauthorized persons to the Software.

5. Term. This license is effective until terminated. You may terminate the license at any time by destroying the Software (including the related documentation) together

with all copies or modifications in any form. Onix Electronic Systems will have the right to terminate your license immediately if you fail to comply with any term or condition of this Agreement. Upon any termination, including termination by you, you must destroy the Software (including all related documentation) together with all copies or modifications in any form.

6. Limited Warranty. Onix Electronic Systems warrants only the media upon which the Software is furnished will be free from defects in material or workmanship under normal use and service for a period of thirty (30) days from the date of delivery to you. ONIX ELECTRONIC SYSTEMS DOES NOT AND CANNOT WARRANT THE PERFORMANCE OR RESULTS YOU MAY OBTAIN BY USING THE SOFTWARE OR DOCUMENTATION. THE FORGOING STATES THE SOLE AND EXCLUSIVE REMEDIES ONIX ELECTRONIC SYSTEMS WILL PROVIDE FOR BREACH OF WARRANTY. EXCEPT FOR THE FOREGOING LIMITED WARRANTY, ONIX ELECTRONIC SYSTEMS MAKES NO WARRANTIES, EXPRESS OR IMPLIED, AS TO NONINFRINGEMENT OF THIRD PARTY RIGHTS, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow the exclusion of implied warranties or limitations on how long an implied warranty may last, so the above limitations may not apply to you. This warranty gives you specific legal rights and you may also have other rights which vary from state to state.

7. Limitations of Liability. IN NO EVENT WILL ONIX ELECTRONIC SYSTEMS BE LIABLE TO YOU FOR ANY SPECIAL DAMAGES, INCLUDING ANY LOST PROFITS, LOST SAVINGS OR OTHER INCIDENTAL OR CONSEQUENTIAL DAMAGES, EVEN IF ONIX ELECTRONIC SYSTEMS HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES, OR FOR ANY CLAIM BY ANY OTHER PARTY. Some states do not allow the exclusion or limitation of special, incidental, or consequential damages, so the above limitation or exclusion may not apply to you.

8. Limitation of Remedies. Onix Electronic Systems' entire liability and your exclusive remedy shall be: (a) the replacement of any media not meeting Onix Electronic Systems' limited warranty which is returned to Onix Electronic Systems; or (b) if Onix Electronic Systems or its distributors is unable to deliver replacement media which is free of defects in material or workmanship, you may terminate this Agreement by returning the Software and your money will be refunded.

9. Export. You acknowledge that the laws and regulations of the United States restrict the export and re-export of the Software. You agree that you will not export or re-export the Software or media in any form without the appropriate United States and foreign government approval.

10. Government Restricted Rights Legend for Units of the DOD. Use, duplication or disclosure by the Government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at 252.227-7013. Onix Electronic Systems Inc., 717 Old Trolley Rd Ste 6 #163, Summerville, SC 29485.

Contents

Chapter 1

Introduction

1.1   Conventions used in this manual

- Names of keys are shown in <>. For example, <TAB>, <ENTER>, <SHIFT>, and <CTRL>.

- Certain actions require the simultaneous use of multiple key strokes. For example, <CTRL>+<A> means that you must hold down the Control key while you press the A key.

- Certain functions are to be performed from the command line. The command to be types will be displayed in the Courier font. For example, type `cat /etc/hosts`, means to type 'cat /etc/hosts' from the command line.

- Some programs such as rtview require cursor navigation. This is performed with the arrow keys. Up arrow will go up a line, and down arrow will go down one line. If there are more ports defined than can fit on the screen, the Page Up and Page Down keys can be used to go a page up and a page down respectively. Also the Home and End keys can be used to go to the first entry on the screen and the last entry on the screen respectively.

- Any time you see a line ending with \, it is a continuation line. You may see these in a configuration file listing. It means that the line should be entered as a complete line without pressing <ENTER> between the lines. There may be more than one line ending with \ if the line is very long.

1.2   Functional Overview

The Internet Paging Terminal (IPT) is our replacement for the ISI and IPG. It merges the functionality of both into one device to provide more options for our customers. The IPT accepts packets from a serial or network connection and delivers them based on a configurable routing table.

1.3   Features and Benefits

- Optional paging encoder.

- Supports Two-tone and Five-tone tone only and voice paging.

- Supports Pocsag, Golay and Flex Tone only, Numeric and Alphanumeric paging.

- Paging traffic received using an open protocol based on TNPP over a network connection so the encoder can be located near your transmitter (or link transmitter).

- Supports receiving messages via SMTP (Internet e-mail), SNPP (Internet network paging), HTTP (Web paging), TAP (Telocator Alphanumeric Protocol), TNPP (Telocator Network Paging Protocol - ID or CAP page), and WCTP (Wireless Communications Transfer Protocol).

- Supports voice paging when paired with an Omega UMS.

- SSL support for HTTP and WCTP

- support TAP and TNPP over the network

1.4   Support Services

If you have any questions about the IPT, please refer to this manual first.

The support email address listed in the beginning of this manual is the best way to contact us for non-emergency technical support.

If you cannot find the answer, contact technical support at the following numbers. High quality, responsive technical support is available 24 hours a day, 7 days a week, including holidays.

For technical support between the hours of 8:30 AM and 4:30 PM Eastern Time, Monday through Friday, excluding holidays, call 843-821-6888. For technical support outside of normal business hours or on holidays, call 843-821-6888. The voice mail operator will answer your call. This number allows you to leave a message for normal business matters, or initiate a page for immediate technical support. The voice mail attendant will lead you through the appropriate procedures. For matters that do not require an urgent response, leave a voice mail message within the general mailbox.

For urgent matters that require that you speak to an on-call technician, select the appropriate key identifying the product for which you need technical support. After the technician's greeting, leave a short message with the area code and phone

number at which you can be reached. The on-call technician will be paged and will return your call.

Phone:	843-821-6888
Fax:	843-821-6894
Web:	`http://harktech.com`
Sales email:	sales@harktech.com
Support email:	support@harktech.com

Chapter 2

Installation

The IPT will already be installed and configured for a basic system. All that is required for initial setup is to plug in the network connection and assign the IP address and network settings.

2.1   Hardware

The Hark Internet Paging Terminal comes in a 1U and 3U rackmount configuration. Both systems have no moving parts such as fans or hard drives that can wear out and fail. They also both run the same software code. The only difference is the expandibility and some options available in the 3U system.

Both systems have a console port for local configuration through an RS-232 port and a network connection for traffic and remote administration. The console port is wired the same as an RS-232 port on a PC. So if you are connecting to a PC you will need a null-modem cable. Over time different CPU boards have been used. The easuest way to differentiate is by the MAC address. See the table below for console serial port settings.

MAC Address	Settings	CPU
00:50:C2:B9:6x:xx	115200 N-8-1	Hark
00:50:C2:97:4x:xx	57600 N-8-1	Cirrus 9307
00:50:C2:C9:2x:xx	115200 N-8-1	Atmel 9G45
00:50:C2:D6:2x:xx	57600 N-8-1	Cirrus 9307
08:00:20:0F:Cx:xx	115200 N-8-1	Ti 3517

2.1.1   IPT-1U

The IPT-1U is a 1U rackmount system that runs off a small 5V power supply. A 5V wall wart is included with the system. This system is for systems that do not need a lot of expandability.

The IPT-1U supports four RS-232 ports. The serial ports are wired the same as a PC DB-9 so a standard DB-9 to DB-25 serial cable can be used to connect to modems. Units with serial number 100504003 and lower support modem handshaking signals on the bottom two ports only. The top two ports have TX, RX, and Ground. Units with serial number 100505001 and higher have full modem control on all four ports. If you want to use modems on the serial ports you must have one of the newer units.

Back panel serial port layout serial numbers with MAC address of 00:50:C2:b9:60:0x:

3: /dev/ttyS4	4: /dev/ttyS5
1: /dev/ttyS2	2: /dev/ttyS3

Back panel serial port layout for all others:

2: /dev/ttyUSB1	4: /dev/ttyUSB3
1: /dev/ttyUSB0	3: /dev/ttyUSB2

An optional built-in modem is supported for dial backup and other uses. Boards with serial number 100505001 and higher also support cellular modems in addition to regular POTS line modems.

An optional built-in paging encoder is also supported for connecting directly to a paging transmitter or to a link transmitter.

The following is the pinout for the DB-25 connecter for systems with a built in encoder:

Pin	Description
1,14	Audio 600ohm transformer
2,15	Digital TTL levels (15=Ground reference)
3,16	Digital RS232 levels (16=Ground reference)
4,17	Key contact closure (Bit0)
5,18	Key contact closure (Bit1)
6,19	Busy in, can be strapped for contact closure, voltage input or common collector ground
7,20	Audio 600ohm transformer
8,21	Digital TTL levels (21=Ground reference)
9,22	Digital RS232 levels (22=Ground reference)
10,23	Key contact closure (Bit2)
11,24	Key contact closure (Bit3)
13,25	Calibrate Switch
15,16,21,22	Ground

We now also offer an 8-port Audio Distribution Board with individual gain settings for all 8-ports.

2.1.2   IPT-3U

The IPT-3U is a 3U rackmount system that uses a backplane for adding additional line cards. The backplane uses USB for the transport method for flexibility and hot-swap. Up to 12 line cards are supported. Currently a four-port modem card and a four-port serial card are available. The four-port modem card can be optionally configured with voice modems to support numeric paging (i.e. remote trunk concentrator). In addition the system supports one or two power supplies. The power supplies are also hot-swappable in the redundant system. The power supplies are 48VDC input only so an external 48V power supply will be needed for compatibility with 110VAC sites.

RS-232 input card

The RS-232 input card contains four serial ports with full modem control. These ports may be configured for incoming or outgoing connections and support the GCP, TAP, and TNPP protocols. Below is the pin-out for the four RJ-45 connectors on the front of the card:

Pin	Function
1	RTS
2	DTR
3	GND
4	TXD
5	RXD
6	DCD
7	DSR
8	CTS

This pinout allows the port to be looped back using a flat "silver-satin" cable with the RJ-45 connectors crimped in a telephone configuration (crossed) as opposed to a typical data configuration (straight-through).

POTS Modem

The standard modem card contains four Multitech Socket Modems. These modems may be from 2400 baud up to 56k. The Tip and Ring connections are brought to the rear of the IPT using RJ-21X connectors. Below is the pinout for the RJ-21X connectors:

J1				
Pair	Pins	Description	Colors	Slot - Channel
1	1,26	R1,T1	Blue/White,White/Blue	1 - 1
2	2,27	R2,T2	Orange/White,White/Orange	1 - 2
3	3,28	R3,T3	Green/White,White/Green	1 - 3
4	4,29	R4,T4	Brown/White,White/Brown	1 - 4
5	5,30	R5,T5	Slate/White,White/Slate	2 - 1
6	6,31	R6,T6	Blue/Red,Red/Blue	2 - 2
7	7,32	R7,T7	Orange/Red,Red/Orange	2 - 3
8	8,33	R8,T8	Green/Red,Red/Green	2 - 4
9	9,34	R9,T9	Brown/Red,Red/Brown	3 - 1
10	10,35	R10,T10	Slate/Red,Red/Slate	3 - 2
11	11,36	R11,T11	Blue/Black,Black/Blue	3 - 3
12	12,37	R12,T12	Orange/Black,Black/Orange	3 - 4
13	13,38	R13,T13	Green/Black,Black/Green	4 - 1
14	14,39	R14,T14	Brown/Black,Black/Brown	4 - 2
15	15,40	R15,T15	Slate/Black,Black/Slate	4 - 3
16	16,41	R16,T16	Blue/Yellow,Yellow/Blue	4 - 4
17	17,42	R17,T17	Orange/Yellow,Yellow/Orange	5 - 1
18	18,43	R18,T18	Green/Yellow,Yellow/Green	5 - 2
19	19,44	R19,T19	Brown/Yellow,Yellow/Brown	5 - 3
20	20,45	R20,T20	Slate/Yellow,Yellow/Slate	5 - 4
21	21,46	R21,T21	Blue/Violet,Violet/Blue	6 - 1
22	22,47	R22,T22	Orange/Violet,Violet/Orange	6 - 2
23	23,48	R23,T23	Green/Violet,Violet/Green	6 - 3
24	24,49	R24,T24	Brown/Violet,Violet/Brown	6 - 4
25	25,50	R25,T25	Slate/Violet,Violet/Slate	CPU Module Modem

J2				
Pair	Pins	Description	Colors	Slot - Channel
1	1,26	R1,T1	Blue/White,White/Blue	7 - 1
2	2,27	R2,T2	Orange/White,White/Orange	7 - 2
3	3,28	R3,T3	Green/White,White/Green	7 - 3
4	4,29	R4,T4	Brown/White,White/Brown	7 - 4
5	5,30	R5,T5	Slate/White,White/Slate	8 - 1
6	6,31	R6,T6	Blue/Red,Red/Blue	8 - 2
7	7,32	R7,T7	Orange/Red,Red/Orange	8 - 3
8	8,33	R8,T8	Green/Red,Red/Green	8 - 4
9	9,34	R9,T9	Brown/Red,Red/Brown	9 - 1
10	10,35	R10,T10	Slate/Red,Red/Slate	9 - 2
11	11,36	R11,T11	Blue/Black,Black/Blue	9 - 3
12	12,37	R12,T12	Orange/Black,Black/Orange	9 - 4
13	13,38	R13,T13	Green/Black,Black/Green	10 - 1
14	14,39	R14,T14	Brown/Black,Black/Brown	10 - 2
15	15,40	R15,T15	Slate/Black,Black/Slate	10 - 3
16	16,41	R16,T16	Blue/Yellow,Yellow/Blue	10 - 4
17	17,42	R17,T17	Orange/Yellow,Yellow/Orange	11 - 1
18	18,43	R18,T18	Green/Yellow,Yellow/Green	11 - 2
19	19,44	R19,T19	Brown/Yellow,Yellow/Brown	11 - 3
20	20,45	R20,T20	Slate/Yellow,Yellow/Slate	11 - 4
21	21,46	R21,T21	Blue/Violet,Violet/Blue	12 - 1
22	22,47	R22,T22	Orange/Violet,Violet/Orange	12 - 2
23	23,48	R23,T23	Green/Violet,Violet/Green	12 - 3
24	24,49	R24,T24	Brown/Violet,Violet/Brown	12 - 4
25	25,50	R25,T25	Slate/Violet,Violet/Slate	Unused

DID Modem

The DID modem card supports up to 2400 baud and also allows DTMF numeric paging on the same line. The subscriber database is used to know whether to answer the call with modem or prompt for digits. The Tip and Ring connections are brought to the rear of the IPT using an RJ-21X connector. See the POTS Modem above for RJ-21X pinout. The DID modem uses special initstring formats. A typical modem entry for the DID modem is as follows:

```
in-did|ATDBG=0|ATCFG=7,5000,3000,250,500,500,2000,4000,10,y|1|0|0|45000
```

ATDBG=0 turns off debugging. The ATCFG= command has several comma seperated fields. They are listed below in order of apperance.

   DID Digits   The number of DID digits expected.

DTMF Timeout	The timeout for entering the first overdial digit on numeric pages.
DTMF IDT	The timeout for entering additional overdial digits.
DID Wink Time	If non-zero, winkstart protocol is used with the wink time defined in ms.
Seize Qualify	The time required to debounce and detect a call start seizure in ms.
Hangup Qualify	The time required to debounce and detect a call end, or hangup in ms.
Ring On Time	The time to generate ringing signal on modem calls in ms.
Ring Silence	The time beween generated rings on modem calls in ms.
Ring Count	The number of rings to generate on modem calls.
Voice Prompts	Enter 'y' or 'n' to enable or disable voice prompts.

T1 Interface - Under Development

A Quad T1 interface is under development. The timeslots will be dynamically assigned to the available line interfaces.

Digital Modem - Under Development

The digital modem card will contain four digital modem interfaces. These modems will support DTMF numeric paging and up to 2400 baud data modem like the standard modem above. This modem must be used in conjunction with the T1 interface card.

2.2   Operating System

The IPT uses the Linux Operating System. Any commands entered are case sensi-
tive unless otherwise noted. This means that when you see `type Exit` you should
type Exit with an upper-case E and the rest lower-case

2.2.1   Linux

A customized version of OpenEmbedded is used. To access the command line type
`Shell` from the main menu. Command line access is not to be used lightly. You can
seriously affect the operation of the IPT by doing something wrong on the command
line. For this reason the command line is to be used under the direction of Hark
support personnel. Please see the Troubleshooting section for additional tools that
are available from the command line.

2.3   Application

The IPT application comes pre-installed on the system. From time-to-time updates
are made available that may offer new features or possibly bug fixes. Below is the
procedure for upgrading the system. It is recommended that this only be done at
the direction of Hark Systems personel and scheduled ahead of time. Some updates
may require manual editing of configuration files for the update to proceed properly.

Upgrade procedure:

If you have the update copied to a Windows computer with Putty and PSCP in-
stalled use the following:

```
pscp -scp ipt-armv4t-2.26.tar.gz root@ipt.ip.addr:/usr/local
```

Replace ipt-armv4t-2.26.tar.gz with the name of the update file you were sent and
replace ipt.ip.addr with the actual IP address of the IPT box you are updating. Sys-
tems with MAC addresses that start with 00:50:C2:B9:6x:xx use armv5te instead of
armv4t.

Once the file is copied to the IPT perform the following steps to update it:

```
login to IPT as root
type 'Exit' to drop to the shell (Exit is case-sensitive)
type 'cd /usr/local' to change to the installation directory
type 'service ipt stop' to stop the IPT service
type 'tar xzvf ipt-armv4t-2.26.tar.gz' to extract the update
type 'tar xzvf ipt-www-2.26.tar.gz' to extract the html files
type 'service ipt start' to start the IPT service
type 'exit' to logout
```

Chapter 3

Configuration

3.1 System

3.1.1 Network configuration

The network configuration should be performed through the iptconfig utility that is displayed when you first login. You may edit the configuration directly, but make sure you also change the settings in iptconfig. If you don't your next network config update will overwrite the system network files erasing any changes you may have made.

In the IPT, the network configuration is stored in /etc/network/interfaces.

Example DHCP configuration:

```
auto lo
iface lo inet loopback

auto eth0
iface eth0 inet dhcp
```

Example static IP configuration:

```
auto lo
iface lo inet loopback

auto eth0
iface eth0 inet static
  address 10.1.1.1
  netmask 255.255.255.0
  gateway 10.1.1.254
```

To view the network configuration type `ifconfig eth0` from the command line.

3.1.2   DNS server

This setting should also be made using the iptconfig menu. Any changes to the /etc/resolv.conf file will be overwritten if the iptconfig network file update menu is used.

The DNS server is specified in /etc/resolv.conf. The following is an example:

```
search harktech.com
nameserver 10.1.1.254
```

Multiple nameserver lines may be specified. It is recommended to have at least two nameservers.

3.1.3   syslog

Unlike the original ISI, the IPT does not use the syslog facility much. It is still built in, but mostly only errors and system warnings are sent to syslog. The debug information is now sent to files in the /var/log/debug directory. See the "Troubleshooting" chapter for more information.

In order to view the syslog from the main menu the /etc/syslog.conf file may need to be modified.

Here is a default syslog.conf:

```
DESTINATION="buffer"            # log destinations (buffer file remote)
REDUCE=no                       # reduced-size logging
BUFFERSIZE=64                   # buffer: size of circular buffer [kByte]
LOGFILE=/var/log/messages       # file: where to log
ROTATESIZE=32                   # file: rotate log if grown beyond X [kByte] (busybox 1.2+)
ROTATEGENS=1                    # file: keep X generations of rotated logs (busybox 1.2+)
REMOTE=loghost:514              # remote: where to log
FOREGROUND=no                   # run in foreground (don't use!)
```

Change the file so it looks like this:

```
#DESTINATION="buffer"           # log destinations (buffer file remote)
DESTINATION="file"              # log destinations (buffer file remote)
REDUCE=no                       # reduced-size logging
BUFFERSIZE=64                   # buffer: size of circular buffer [kByte]
LOGFILE=/var/log/messages       # file: where to log
ROTATESIZE=1024                 # file: rotate log if grown beyond X [kByte] (busybox 1.2+)
ROTATEGENS=1                    # file: keep X generations of rotated logs (busybox 1.2+)
REMOTE=loghost:514              # remote: where to log
FOREGROUND=no                   # run in foreground (don't use!)
```

Basically we copied the first line and pasted it. Next the first line was commented and the buffer in the second line was changed to file. This will cause the syslog messages to be written to a file named /var/log/messages in the system's RAM disk. We also changed the ROTATESIZE from 32 to 1024.

After changing the syslog.conf file the syslog server needs to be restarted by typing the following:

```
service syslog stop
service syslog start
```

3.2 Clustering

IPT version 1.7 support hot-standby systems with IP address take over. Two identically configured machines will communicate with each other over a null-modem cable. Typically port 4 on both machines will be configured for the HEARTBEAT protocol.

If the primary machine can no longer ping the gateway, it will ask the standby machine over the RS-232 cable to take over. If the standby machine can ping the gateway it will accept the take over request. The primary machine will then release the virtual IP address and tell the standby machine to go ahead and take the IP address. If the standby machine also can not reach the gateway it will refuse the take over request and the primary will continue to ping the gateway and also issue take over requests to the standby (in case the standby connection to the gateway becomes available first).

The standby machine is also continually checking the gateway and the primary machine. If it can not reach the primary machine and it can not ping the virtual IP but it can still reach the gateway it will add the virtual IP to its interface and takeover services. This configuration means that if the RS-232 cable becomes unplugged, but it can still reach the virtual IP over the network it will assume that the cable became unplugged and the primary is still operational so it will remain in standby.

3.3 Application

The menu below is displayed when first logging in. The Server status section will only display on systems configured for hot-standby. The system architecture is now displayed after the version number. This is for determining which update to use. The

archives will either be armv4t or armv5te. The architecture shown below, armv5tejl, is abbreviated as armv5te.

```
 IPT version...: 2.26 armv5tejl
 Host name.....: ipt.harktech.com (Please update hostname)
 eth0..........: 00:50:c2:c9:2b:c6 10.100.1.8/255.255.255.0
 eth1..........: 00:50:c2:b9:60:16 10.100.1.28/255.255.255.0
 Date/time.....: 2010-05-13 23:34:39 TZ=EST5EDT,M3.2.0/2,M11.1.0/2
 Server status.: VIRTUAL 10.100.1.10
                 PRIMARY 10.100.1.8 us
                 STANDBY 10.100.1.9 reachable


 1) View Syslog
 2) View Real-time Stats
 3) Edit Routing Entries
 4) Edit Profiles
 8) System Utilities
 9) System Configuration

Enter selection (or L to Log Off):
```

3.3.1   View Syslog

This requires that the syslog entries are sent to a file. See the syslog section in the "Configuration" chapter for more information. To view the Linux system log (syslog) enter 1 from the main menu. You will see the following:

```
 **************************************
 ***  Viewing system log (syslog).  ***
 ***        Type exit to exit.       ***
 **************************************
```

Type exit and press <Enter> to exit the syslog viewer and return to the menu.

We no longer send many application messages to syslog so there probably won't be any useful troubleshooting information in there for the IPT application. However, the system messages will still go to syslog.

3.3.2   View Real-time Stats

Real-time port statistics can be viewed by selecting option 2 from the main menu. The following is an example of the real-time stats:

```
Port          Status Number      Function      Remote IP        RxAccept RxReject
gcp           RUNNING                                                  0        0
http          RUNNING                                                  1        0
smtp          RUNNING                                                  0        0
snpp          RUNNING                                                  0        0
tap           RUNNING                                                  0        0
tnpp          RUNNING                                                  0        0
purgedebug    RUNNING                                                  0        0
monitor       RUNNING          UP            10.100.1.254             0        0
ev/ttyUSB0    RUNNING          TAP IDLE                                0        0
ev/ttyUSB1    STOPPED                                                  0        0
ev/ttyUSB2 FAULTOFF                                                    4        0
ev/ttyUSB3     START                                                   0        0
ev/ttyUSB4    RUNNING          TAP IDLE                                0        0
1.100:1234    STOPPED                                                  0        0
1.100:1235    STOPPED                                                  0        0
```

To exit real-time stats press 'q' to quit. You may use the arrow keys to move up and down. For the network threads (gcp, http, smtp, snpp, tap, tnpp) you may press the right arrow to get more detailed stats for the protocol. You may stop individual threads (ports) by pressing <F6> and start them with <F7>.

3.3.3   Edit Routing Entries

The IPT uses a combination of number ranges and subscriber records to control how a message is delivered. The number ranges are called idblocks. Most systems can be configured purely by idblock. The system is setup with a number range that takes any number in that range and then sends it using another paging protocol. The number may be modified in some way like prefixing and area code if the receiving system is expecting 10 digits and the IPT is only receiving 7 digits. The number can also be modified by stripping the area code if the IPT is receiving 10 digits and receiving system only supports 7. The 7 and 10 are used as examples here. The number to be prefixed and/or stripped may be from 1 to 16 digits.

The idblock ranges can be maintained by selecting option 3 from the main menu. The following is the idblock menu:

```
Idblock maintenance menu

 (A)dd Idblock Entry
 (M)odify Idblock Entry
 (D)elete Idblock Entry
 (L)ist idblock entries
 (Q)uit and save changes
 e(X)it without saving changes


Enter selection:
```

The first thing you should do on new systems is select 'L' to list the existing number ranges. You will probably want to delete or modify the default number range.

3.3.4   Edit Profiles

The IPT uses various profile definitions to reduce redundant settings. This decreases the size of the ini file and makes the system easier to setup by not having to re-enter information for multiple ports.

```
Profile menu

 1) Passthrough profiles
 2) TAP profiles
 3) TNPP profiles
 4) Destination profiles
 5) Encoder profiles
 6) Fivetone profiles
 7) Golay profiles
 8) Pocsag profiles

10) Twotone profiles
11) Zone profiles

Enter selection (or Q to quit):
```

Passthrough profiles

Passthrough profiles define the values used by passthrough ports. Passthrough ports are the original ISI ports that take serial traffic and transport it over the network.

The system ships with a default passthrough profile that can be customized or additional profiles may be added. The profiles can also be listed to see the values used by default.

TAP profiles

TAP profiles define the values used by TAP ports. These are used for direct RS-232, modem, and network TAP ports.

The system ships with a default TAP profile that can be customized or additional profiles may be added. The profiles can also be listed to see the values used by default.

TNPP profiles

TNPP profiles define the values used by TNPP ports. These are used for direct RS-232, modem, and network TNPP ports.

The system ships with a default TNPP profile that can be customized or additional profiles may be added. The profiles can also be listed to see the values used by default.

Destination profiles

Destination profiles define the values used for outgoing messaging.

The system ships with a set of default destination profiles that can be customized or additional profiles may be added. The profiles can also be listed to see the values used by default.

Encoder profiles

Encoder profiles define the values used by encoder ports.

The system ships with a default encoder profile that can be customized or additional profiles may be added. The profiles can also be listed to see the values used by default.

There are also profiles for the different encoder formats. These include POCSAG, Golay, Fivetone, and Twotone. There is also a profile for zones. These are all related to the paging encoder. If you do not have the optional built-in paging encoder, you don't need to worry about these settings.

3.3.5   System Utilities

3.3.6   System Configuration

3.4   ipt.ini

This is the main configuration file. It is structured like a Microsoft Windows ini file. There is a common section which applies to all programs and a section for each area of the application. Refer to the "Program Descriptions" chapter for more information on the programs referred to in this section.

3.4.1 [common]

Common settings for all programs.

DEBUG_LEVEL	Sets the amount of debugging information logged to the debug directory. The following is a list of the values for each type of information that can be logged. Add the values together for the value to set the DEBUG_LEVEL.

0x00000000	No debug
0x00000001	Logging (a lot of miscellaneous debug info)
0x00000002	Functions (log entering functions)
0x00000008	Queues
0x00000010	Semaphores
0x00000020	ComLib (log serial port calls and info)
0x00000040	NetLib (log network calls and info)
0x00000080	Read
0x00000100	Write
0x00001000	Tap Library logging
0x00002000	Tnpp Library logging
0x00004000	Thread information
0x00008000	Telephony switching
0x00010000	Web page template parsing
0x00020000	Log reads of zero bytes also (not recommended)
0x00040000	write billing logs
0x00080000	Message data (may create extremely large files)
0x00100000	decode mime
0x00200000	bin2str
0x00400000	Modem capabilities
0x00800000	HTTP admin sessions (not recommended)
0x01000000	Database open/close
0x02000000	Parse line
0x04000000	Interprocess communication
0x08000000	Trim silence

MASQUERADE_AS	Fully qualified host name to masquerade as when sending email. For example, if your domain name was example.com and your published hostname is pager.example.com, but the Omega's hostname is omega1.example.com. Enter pager.example.com for this field and all email will look like it came from pager.example.com not omega1.example.com. This field may be up to 80 characters long.

HELO_NAME   Enter the name returned by an nslookup on the
                            system's IP address. This field is used to lower
                            the Spamassassin score on outgoing emails. This
                            is recommended if your forward and reverse DNS
                            do not match. For example, your machine is called
                            pager.example.com and the reverse DNS for your
                            machine's IP address returns something like rrcs-
                            123-234-123-234.midsouth.biz.rr.com. This field
                            may be up to 80 characters long.

LICENSE_KEY   The license key for this system. As of version 1.7
                            two license key/feature key pairs are supported
                            for hot-standby systems. As of version 2.30, this
                            value resides in files located in the license.d direc-
                            tory. This is provided to allow easier copying of
                            the ini file from one machine to another. Also, all
                            files in the license.d directory are scanned until a
                            valid license is found.

FEATURE_KEY   Specifies the licensed features for this system. As
                            of version 2.30, this has been moved to files lo-
                            cated in the license.d directory.

RLIMIT_MSGQUEUE   The maximum number of bytes allowed for all
                            message queues opened by the real user id of the
                            process. Typical Linux default is 819200. This
                            value may need to be raised if there are many
                            SMPP and TNPP threads or many TAP output
                            threads. The maximum value currently allowed in
                            the ipt is 67108864 (64 megabytes). Shortcuts are
                            supported. For example, the M suffix can be used
                            for Megabytes and G for Gigabytes. To specify 64
                            megabytes, you can use 64M.

THREAD_STACK_SIZE	Allows modifying the default stack size when a thread is created. This should be set to at least 262144. Shortcuts are allowed, so 262144 can also be entered as 256k.
SMART_HOST	This points to the external email server that will be used to send all outgoing mail.
SMARTHOST_TIMEOUT	The timeout allowed to wait for responses from the email server.
EMAIL_FROM	The from address to use for outgoing emails if there is no from address on the incoming message. For example, if the message is received via TNPP.
EMAIL_SUBJECT	The subject to use for outgoing emails if there is no subject on the incoming message.
EMAIL_FORMAT	0=concatenate lines of incoming email together separating each with a space. 1=each line of incoming email sent as separate line separated with a line feed
EMAIL_PREFIX_FROM	Prefix the email from address with this text. Only used if the sendfields are set to send the from and other fields are also sent.
EMAIL_PREFIX_TO	Prefix the email to address with this text. Only used if the sendfields are set to send the to and other fields are also sent.
EMAIL_PREFIX_SUBJECT	Prefix the email subject with this text. Only used if the sendfields are set to send the subject and other fields are also sent.
EMAIL_PREFIX_BODY	Prefix the email body with this text. Only used if the sendfields are set to send the body and other fields are also sent.
RETRY_MAX_RETRIES	The maximum number of retries if the message send fails. This may be a value from 0 to not retry to 10 for 10 retries. A value of 2 is typical.

RETRY_INTERVAL	The amount of time in seconds to wait before retrying a failed message send. This may be 0 for no wait to 600 for a 10 minute wait. Long wait times are not recommended as they will cause a delay before a response is sent to the message originator. This value is typically set to 1 to wait 1 second between tries.
DEFAULT_THROTTLE	Specifies the default throttle number. Set to 0 to disable recipient throttle checking. Otherwise select one of the records in the throttle table for a default to use for everyone that does not have a throttle number specified in their settings. See the throttle table in the Database Chapter for more information.
MAX_FROM_LENGTH	The maximum length of the email from address to use in the outgoing message. Unlike the Omega systems, setting this value to 0 will prevent the From header from being prefixed to the message.
MAX_SUBJECT_LENGTH	The maximum length of the email subject to use in the outgoing message. Unlike the Omega systems, setting this value to 0 will prevent the Subject header from being prefixed to the message.
MAX_MESSAGE_LENGTH	The maximum length of incoming messages. Any messages longer than this are truncated on input.
ALLOW_DOMAINS	A comma-separated list of domains for which we accept messages.
IP_ALLOW	A list or range of IP addresses that are allowed to connect and send to us. Leave empty or 0.0.0.0 to allow all connections.
PURGE_DEBUG_DAYS	Specify the number of days to retain the debug logs. The debug logs are stored in a tmpfs filesystem which has limited space. The reason tmpfs is used is so that the flash memory is not written to constantly using up the number of write cycles the flash supports. The debug logs are stored in /var/log/debug/YYYY-MM-DD.

PURGE_DEBUG_HOUR	Specify the hour of the day to purge the debug logs.
ARCHIVE_DEBUG_INTERVAL	
	This specifies how often debug files are moved to an archived path like a USB attatched thumb drive. The value is in seconds. When this threshold is reached, the debug file is moved to the archive path and a new local file is created in the tmpfs.
ARCHIVE_DEBUG_SIZE	This specifies a size threshold used for archiving local debug files. This value is in bytes. When an individual debug file hits this threshold, it is moved to the archive path and a new local file is created in the tmpfs.
ARCHIVE_DEBUG_PATH	This specifies the path to the archive file structure. Files are moved here when the INTERVAL or SIZE thresholds are met to help manage the size of the tmpfs used by debug files.
STRIP_PLUSONE	Strip the 1 from the front of an 11-digit number that starts with 1.
RANDOM_DEVICE	Specify the device to use for random numbers. This is typically PRNG.
BROADCAST_SEND	IPT version 1.6 and higher has the ability to send an identical packet out one or more ports. For now this is limited to GCP output.
SYSTEM_IDENTIFIER	This is a descriptive identifier used to identify this system in log files.
BILLING_LOG	This enables/disables the billing logs. They default to /usr/local/logs/YYYYMMDD.log.
SNTP_SERVER	This specifies the SNTP server and enables the IPT to use an SNTP server to keep its time in sync with network time.

SNTP_INTERVAL	This specifies the interval used for SNTP updates. The time is specidied in seconds.
TUNNEL_USER	This is the MAC ADDRESS (all uppercase) of Eth0 without the colons. This is used by menu option 8-12 to open up a reverse SSH tunnel.
TUNNEL_PORT	This is the port number to use when setting up a reverse tunnel connection. For the 1U-ipt, this is calculated buy taking the last three hex digits of the TUNNEL_USER, converting it to decimal and adding 50000.

3.4.2   [destprofile]

Destination profiles consist of a single line per profile. Each line contains the various settings for the profile. There are two separate formats for the destination profile line. One for serial destinations and one for network destinations. The fields for the two types are:

```
Serial:
number|name|enabled|1|protocol|option|comport|idformat|maxlen|tries|
mdmtype|mdmnum|baud|parity|databits|stopbits

Network:
number|name|enabled|2|protocol|option|hostname|portnum|idformat|maxlen|tries|
username|password|connecttimeout

ENCODER connections add the following to the end:
channel|zone|tnppdest|inertia

SMS adds sourceaddr to the end.

TAP adds tappassword to the end.

TNPP connections add the following to the end:
tnppdest|channel|zone|inertia
```

Number is the profile number to use in the primarydestprofile and/or backupdest-profile in each routing entry. Name is a description for the profile. Enabled is whether the profile is allowed to be used for destinations or not. The next field is 1 for serial connections or 2 for network connections. Protocol may be ENCODER, GCP, SMS, TAP, or TNPP for serial connections or SMPP, SMTP, SNPP, WCTP or WCTPS for network connections.

Starting in version 2.12 there is now a protocol option field immediately after the protocol field. This specifies any special options required for this connection. Currently only specifying the WCTP submit type and encoder options support protocol options. This uses the same protocol options as the incoming protocols. In order to support sending wctp-SubmitRequest instead of the default wctp->SubmitClientMessage set the option field to 0x00000020 (decimal 32). This value may be specified in either hex or decimal. The encoder options are configured as follows:

0x00000000	No options
0x00000001	Enable Pocsag
0x00000002	Enable Golay
0x00000004	Enable 2 Tone (tone only)
0x00000008	Enable 5 Tone (tone only)
0x00000010	Enable Voice (not supported)
0x00000020	Enable Raven (proprietary)
0x00000040	Enable Flex
0x40000000	Enable Simplex (for ATC only)
0x80000000	Output to ATC

Serial connections specify the comport (e.g. /dev/ttyS1 or /dev/ttyUSB0). The comport is followed by the idformat (e.g. %10i), the maximum message length, the number of tries, the modemtype (one of the modems listed in the [modem] section or none for direct connections), the modem number (or none for direct connections), baud, parity, databits, and stopbits.

Special notes concerning setting up an ATC destination: The ATC uses TNPP as a transport layer which uses the tnppdest field, so set the comport to /dev/null, set the tnppdest to the destination required, and set the inertia needed to reach the end TNPP node for the ATC. A port entry must also exist with a DEVICE_NAME of /dev/null and a PROTOCOL entry set to ENCODER. This port needs a PROFILE entry pointing to the proper encoderprofile. Also, a corresponding tnpproute entry must exist that matches the tnppdest field. Its device field must also match a port entrie's DEVICE_NAME with a protocol set for TNPP and its PROFILE entry pointing to the proper tnppprofile to complete the connection to the ATC. The tnppdest and inertia fields are ignored if the ATC bit is not set in the option field described above.

Network connections specify the remote hostname (or IP address), the remote port number, the idformat, maximum message length, the number of tries, and an optional username and password for SNPP, WCTP, and WCTPS connections. Starting in version 2.6 network connections also support a connect timeout. This is a

maximum amount of time in milliseconds to wait for the NetClientOpen routine to connect. This only affects regular network connections and is not currently supported for SSL connections.

The idformat allows certain formatting variables to specify how the incoming pager ID is formatted for output. For example, if your TAP output expects 7 digits, use %7i. The caller can send 7 or more digits in the ID and this will take the last 7 digits of the id for the output. If your callers typically send 7 digits and your paging terminal expects 10 digits you may prefix a number. For example, to prefix 843 use 843%7i. The 7 used in these examples can be other values. Some typical values are 4, 5, or 10. maxlen is the maximum number of characters to send in a message. maxtries is the maximum number of attempts before trying the backup destination if one exists. mtype is the modem type as defined in the modem section. This field is case-sensitive. Make sure that you use lower-case names like in the modem section. If this is a direct connection specify none for the modem type. dial is the modem number to dial. If this is a direct connection specify none for the number to dial. baud, parity, dbits, and sbits are the communication settings for the modem. Typically you will only change the baud rate as the TAP protocol specifies that the data bits will be 7 with even parity and one stop bit, and TNPP specifies that the data bits will be 8 with no parity and one stop bit. You do need to specify all of the values though.

The backup destination allows the message to be sent to another destination if the primary is down.

3.4.3   [dnsbl]

This section is not formatted like a typical ini file section. Multiple records are supported in this section and the fields are all specified on one line with a vertical bar (|) separating the values. The dnsbl fields are:

```
hostname|enabled|string
```

The hostname is the DNS-based blocklist to use. Enabled specifies whether or not to use this list for checking if a message is spam and string specifies the return string to send to clients if their message is not accepted.

3.4.4   [ethernet]

This section stores our copy of the network settings. Changes are made to the ethernet settings through the main menu and stored in the ini. There is an option in the "System Utilities" menu to update the system network files and restart the

network interfaces. Starting with version 2.0 this section holds the settings for both the primary and the standby machines when used in a hot-standby configuration. This is done so that it is easier to maintain the configuration. For example, the primary system ini can be modified and then just copied to the standby system without having to repeat your changes on the second machine.

PRIMARY_MODE	The primary server's ethernet mode. This may be set to either the number or text value. 0=DISABLED, 1=STATIC, 2=DHCP. DISABLED is not normally used as the IPT should always be connected to the network. If the IPT is to be used as a server STATIC should be used. The exception to this is if you statically assign IP information using DHCP. DHCP can be used for statically assigning the address, gateway, and DNS settings or can be used for a dynamic IP if the IPT is being used as an ISI converting serial input protocols (GCP, TAP, TNPP) to outgoing Internet protocols such as SNPP or WCTP.
PRIMARY_MAC	The primary server's MAC address. This is required and can be found on the sticker on the back of the unit. It is also displayed on the menu after logging in. This will be set from the factory and should not require changing.
PRIMARY_HOSTNAME	The primary server's fully qualified host name. This is written to /etc/hostname when the network configuration is updated.
PRIMARY_IP	The primary server's IP address. This is only used for STATIC configurations and may be left blank if using DHCP.
PRIMARY_NETMASK	The primary server's network mask. This is only used for STATIC configurations and may be left blank if using DHCP.
PRIMARY_ETH1_MODE	The primary server's ethernet mode for eth1. This may be set to either the number or text value. 0=DISABLED, 1=STATIC, 2=DHCP. If the IPT is to be used as a server STATIC should be used. The exception to this is if you statically assign IP information using DHCP. DHCP can be used for statically assigning the address, gateway, and DNS settings or can be used for a dynamic IP if the IPT is being used as an ISI converting serial input protocols (GCP, TAP, TNPP) to outgoing Internet protocols such as SNPP or WCTP.

PRIMARY_ETH1_MAC	The primary server's MAC address for eth1. This is required and is displayed on the menu after logging in. This will be set from the factory and should not require changing.
PRIMARY_ETH1_IP	The primary server's IP address for eth1. This is only used for STATIC configurations and may be left blank if using DHCP.
PRIMARY_ETH1_NETMASK	
	The primary server's network mask for eth1. This is only used for STATIC configurations and may be left blank if using DHCP.
STANDBY_MODE	The standby server's ethernet mode. This may be set to either the number or text value. 0=DISABLED, 1=STATIC, 2=DHCP. DISABLED is not normally used as the IPT should always be connected to the network. If the IPT is to be used as a server STATIC should be used. The exception to this is if you statically assign IP information using DHCP. DHCP can be used for statically assigning the address, gateway, and DNS settings or can be used for a dynamic IP if the IPT is being used as an ISI converting serial input protocols (GCP, TAP, TNPP) to outgoing Internet protocols such as SNPP or WCTP.
STANDBY_MAC	The standby server's MAC address. This is required and can be found on the sticker on the back of the unit. It is also displayed on the menu after logging in. This will be set from the factory and should not require changing.
STANDBY_HOSTNAME	The standby server's fully qualified host name. This is written to /etc/hostname when the network configuration is updated.
STANDBY_IP	The standby server's IP address. This is only used for STATIC configurations and may be left blank if using DHCP.

STANDBY_NETMASK

The standby server's network mask. This is only used for STATIC configurations and may be left blank if using DHCP.

STANDBY_ETH1_MODE

The standby server's ethernet mode for eth1. This may be set to either the number or text value. 0=DISABLED, 1=STATIC, 2=DHCP. If the IPT is to be used as a server STATIC should be used. The exception to this is if you statically assign IP information using DHCP. DHCP can be used for statically assigning the address, gateway, and DNS settings or can be used for a dynamic IP if the IPT is being used as an ISI converting serial input protocols (GCP, TAP, TNPP) to outgoing Internet protocols such as SNPP or WCTP.

STANDBY_ETH1_MAC

The standby server's MAC address for eth1. This is required and is displayed on the menu after logging in. This will be set from the factory and should not require changing.

STANDBY_ETH1_IP

The standby server's IP address for eth1. This is only used for STATIC configurations and may be left blank if using DHCP.

STANDBY_ETH1_NETMASK

The standby server's network mask for eth1. This is only used for STATIC configurations and may be left blank if using DHCP.

VIRTUAL_IP

The virtual IP is used for hot-standby systems. This is the IP address that is published for use by the outside world. When running in hot-standby the virtual IP address will move to the active IPT server. Please see the "Clustering" section in the "Configuration" chapter for more information.

VIRTUAL_NETMASK	The network mask to use for the virtual IP address.
GATEWAY	The default gateway for the system.
NAMESERVER1	The primary name server for the system.
NAMESERVER2	The secondary name server for the system.

3.4.5   [encoderprofile]

Settings for the encoder profile. This section specifies multiple values per line. The line format is:

```
number|name|option|stationid|idinterval|idtonedelta|keyupdelay|keydowndelay|
maxkeytime|maxpacket|watchdog|mtonehi|mtonelo|mhilo|datainvert|digitalid|
prebits|pretonegap|pretonetime|pretonefreq|voicealerttime|cor|idlekey|
latency|atcbatchgap
```

number	spcifies the profile number.
name	specifies a discriptive name for the profile.
option	specifies the protocol option bits. 0x00000000 = No options 0x00000001 = Enable Pocsag 0x00000002 = Enable Golay 0x00000004 = Enable 2 Tone (tone only) 0x00000008 = Enable 5 Tone (tone only) 0x00000010 = Enable Voice (not supported) 0x00000020 = Enable Raven (proprietary) 0x00000040 = Enable Flex 0x40000000 = Enable Simplex (for ATC only) 0x80000000 = Output to ATC
stationid	specifies the Station ID that is sent out via morse code on the channel.
idinterval	specifies in seconds how often to send the Station ID.

idtonedelta   specifies the frequency of the morse code tone when not
                       using the digitalid mode.

keyupdelay   specifies the time delay between keyup and the sending
                       of data.

keydowndelay   specifies the time to leave the channel keyed after data is
                       complete.

maxkeytime   if non-zero, this is the maximum time that a paging batch
                       can use. This is for sharing of a frequency with other
                       equipment.

maxpacket   this specifies the maximum packet size that can be sent
                       to the encoder.

watchdog   set to 0, this feature is not curently implemented.

mtonehi   this is the modem frequency used to designate a HI level.

mtonelo   this is the modem frequency used to designate a LO level.

mhilo   this specifies weather modem tones are sent at high or
                       low audio level.

datainvert   if non-zero, this specifies that all data is inverted.

digitalid   if non-zero, station ID is sent digitally using long and
                       short bursts of comma at a certain bitrate. Set to 2, to
                       indicate 1200 baud tone bursts for Station ID.

prebits   if non-zero, this indicates the number of BYTES sent out
                       at 337 baud on the channel before the actual paging be-
                       gins. This is helpful for some pagers to lock on to center
                       frequency without impacting actual paging protocols.

pretonegap   the silence gap in ms used after a pre tone is sent and
                       the actual tone pageing ID's are sent.

pretonetime   the time of the pretone in ms (tone paging only).

pretonefreq   the frequency used for the pretone (tone paging only).

voicealerttime	the time in ms for a pager's voice alert, normally set to 2000 (2 seconds). This is only for tone voice paging.
cor	this specifies the COR active level to indicate that the channel is busy. No paging will occur until the COR signal is no longer detected. This is used when sharing a channel.
idlekey	this indicates the key states to output when the channel is Idle.
latency	this specifies the time in ms it takes for a packet to arrive at the ATC after being sent. Used to specify internet or satelite delays.
atcbatchgap	minimum time between actual paging packets on the RF frequency when using the ATC.

3.4.6   [fivetoneprofile]

Settings for the fivetone profile. This section specifies multiple values per line. The line format is:

```
number|name|timeout|waketime|wakegap|pretime|pregap|tonetime|idtgap|functime|
pagegap|spclrepeat
```

number	specifies the number of the profile.
name	a descriptive name for the profile.
timeout	the que timeout value in seconds. A page will remain in queue for this ammount of time waiting for other pages of the same format. This value is not refreshed by newer pages. A page will go out for this format after the timeout occures if no other previuos pages or queues exist.
waketime	length of a wakeup tone in ms. Used to begin a batch of pages.
wakegap	length of gap between wake tone and actual pageing in ms.

pretime	length of the preamble tone (first tone of each sequence) in ms.
pregap	length of gap after first tone and other digits in ms.
tonetime	length of the remaining tones in ms.
idtgap	length of gap between remaining tones in ms.
functime	length of function time, set to 0.
pagegap	gap between pages in ms.
spclrepeat	if y or non-zero, specifies to repeat the pages.

3.4.7   [golayprofile]

Settings for the golay profile. This section specifies multiple values per line. The line format is:

`number|name|timeout|invert`

number	specifies the number of the profile.
name	a descriptive name for the profile.
timeout	queue timeout value in seconds (see above for more information).
invert	if set to 'y' or non-zero, the golay data is inverted in relation to the standard specified in the encoderprofile's inversion setting.

3.4.8   [pocsagprofile]

Settings for the pocsag profile. This section specifies multiple values per line. The line format is:

`number|name|timeout|512xtracomma|1200xtracomma|2400xtracomma|pad|invert`

number	specifies the number of the profile.

name   a descriptive name for the profile.

timeout   queue timeout value in seconds (see above for more in-
                   formation).

512xtracomma   number of extra bytes (8 bits) of comma to use for 512
                   pager wakup time. These are in addition to the standard
                   comma specified by the pocsag protocol.

1200xtracomma   number of extra bytes of comma to use for 1200 pager
                   wakeup time.

2400xtracomma   number of extra bytes of comma to use for 2400 pager
                   wakeup time.

pad   if non-zero, specifies the minimum number of idle code
                   words to place between pages. This can be used to help
                   force end of page detection in outlying areas.

invert   if set to 'y' or non-zero, the pocsag data is inverted in
                   relation to the standard specified in the encoderprofile's
                   inversion setting.

3.4.9   [ravenprofile]

Settings for the raven profile. This section specifies multiple values per line. The
line format is:

```
number|name|timeout|512xtracomma|1200xtracomma|commabytes
```

number   specifies the number of the profile.

name   a descriptive name for the profile.

timeout   set to 1.

512xtracomma   set to 0.

1200xtracomma   set to 0.

commabytes   set to 650.

3.4.10   [flexprofile]

Settings for the flex profile. This section specifies multiple values per line. The line format is:

```
number|name|timeout|maxcollapsebits|collapsebits
```

number   specifies the number of the profile.

name   a descriptive name for the profile.

timeout   the queue timeout in seconds (see above for more information).

maxcollapsebits   specifies the frame's maxcolapsebits value.

collapsebits   specifies the frame's collapsebits value.

3.4.11   [twotoneprofile]

Settings for the twotone profile. This section specifies multiple values per line. The line format is:

```
number|name|timeout|gap|gaptime|pagegap|atime|btime|grouptime|groupextra
```

number   specifies the number of the profile.

name   a descriptive name for the profile.

timeout   the queue timeout in seconds (see above for more information).

gap   if 'y' or non-zero, a gap is sent before the first twotone page.

gaptime   time of the gap in ms. Default is 200.

pagegap   time of the gap between pages in ms. Default is 250.

atime   time of the first tone of the two-tone page in ms. Default is 1000.

btime   time of the second tone of the two-tone page in ms. Default is 3000.

| grouptime | time of a groupcall tone in ms. Default is 8000. |
| groupextra | set to 1700. |

3.4.12   [zoneprofile]

Settings for the zone protocol. This section specifies multiple values per line. The line format is:

```
number|name|analogkey|digitalkey|guardtone|gtonedelta|purc
```

number	specifies the number of the profile.
name	a descriptive name for the profile.
analogkey	a 4 bit hex value to indicate the key bits to send when sending an analog page. Values can be or'ed. See the following table: 0x01 = Closes KEY0. 0x02 = Closes KEY1. 0x04 = Closes KEY2. 0x08 = Closes KEY3.
digitalkey	a 4 bit hex value to indicate the key bits to send then sending a digital page. See above for more information.
guardtone	Specifies the type of tone paging to use. 0 = no tone paging. Used when direct control of transmitter key and data is being used. 1 = tone keying. Used over a link when the transmitter is tone keyed by a guard tone. 2 = purc tone paging. Use when sending to a transmitter that uses PURC tone key and data.
gtonedelta	Frequency of the guard tone, typically 2175.
purc	Specifies the PURK keying sequence used. This string is made up of tone:time pairs seperated by commas. A typical example is: 2175:120,1950:40. This will send out a 120 ms guard tone and a 40 ms key tone (no knock down tones are specified, so all transmitter zones key). To add knock down tones add them as needed between the guard and key tone pairs.

3.4.13   [gcpd]

Glenayre Computer Protocol server configuration.

DEBUG_LEVEL	Level of debugging information to write to the debug directory. See the [common] section for a description of the values.
LISTEN_PORT	Specifies the port on which to listen. This is a TCP port from 1 to 65535. If 0 is used the port will be disabled.
MAX_QUEUE_ENTRIES	Number of queue entries to allocate for this protocol.
IP_ALLOW	A list or range of IP addresses that are allowed to connect and send to us. Leave empty or 0.0.0.0 to allow all connections.
DEFAULT_PROFILE	The default gcp profile to use if one is not specified in the port definition.
VERSION	The GCP protocol version we report when asked via the @RV or @rv command.

3.4.14 [gcpprofile]

Settings for the gcp protocol. This section specifies multiple values per line. The line format is:

```
number|name|option|buffsize|inittime|sectime|linkinterval|linktries
```

Number is the profile number to use in the port definition.

Name is a description for the profile.

Option specifies the protocol options for this profile.

Buffsize specifies the size of the read buffer. Shortcuts are allowed, so 65536 can also be entered as 64k.

Inittime and Sectime specify the initial and secondary read timeouts. The default value is 10000 and 1000. This is for a 10 second initial read timeout and a 1 second secondary read timeout. The initial read timeout is the amount of time in milliseconds the system waits for data. Once the system starts receiving data the secondary read timeout is used to wait for any additional data.

LinkInterval is the time in seconds between sending <CR>'s and waiting for a
'*' response.

LinkTries is the number of <CR>'s to send attempting to establish a link.

3.4.15 [heartbeat]

This section controls the heartbeat thread network connection testing. This is where
you will enter the IP address and the interval to ping to see if the system needs to
request the standby server to take over. This configuration should be the same on
both systems. If the standby server also can not reach the heartbeat ping address
it will refuse to take over the virtual IP from the primary machine.

PING_INTERVAL	Specify the amount of time in seconds between heartbeat pings to the gateway which are used to determine if the system can reach the network. This field is only used for clustered systems. Leave this field empty for standalone systems. See the "Clustering" section above for more information.
PING_ADDRESS	Specify the IP address for the heartbeat pings. This is typically the default gateway address. This field is only used for clustered systems. Leave this field empty for standalone systems. See the "Clustering" section above for more information.
PING_TIMEOUT	Time to wait for a ping response in milliseconds. The valid range is from 100 to 30000 (30 seconds).
PING_TRIES	Number of attempts to retry a ping before switching to the standby machine. The valid range is from 0 to 10.

3.4.16 [httpd]

HTTP server.

DEBUG_LEVEL	Level of debugging information to write to the debug directory. See the [common] section for a description of the values.

LISTEN_PORT	Specifies the port on which to listen. This is a TCP port from 1 to 65535. HTTP typically uses port 80. If 0 is used the port will be disabled.
BUFFER_SIZE	Specifies the size of the read buffer. This value will be used if one is not specified in the service table for the device. Shortcuts are allowed, so 65536 can also be entered as 64k.
PROTOCOL_OPTION	Specifies the protocol options specific to this protocol.
READ_TIMEOUT	Specifies the initial and secondary read timeouts. The default value is 30000:1000. This is for a 30 second initial read timeout and a 1 second secondary read timeout. The initial read timeout is the amount of time in milliseconds the system waits for data. Once the system starts receiving data the secondary read timeout is used to wait for any additional data.
IP_ALLOW	A list or range of IP addresses that are allowed to connect and send to us. Leave empty or 0.0.0.0 to allow all connections.
SESSION_EXPIRE	The amount of time in minutes before the HTTP session times out.
SHOW_SUBLIST	Show list of subscribers with showinlist enabled in a drop down list on the send web message page.
SHOW_FROM	Show the from box on the send web message page to allow the sender to specify who the message is from.
SHOW_SUBJECT	Show the subject box on the send web message page to allow the sender to specify a subject.
SHOW_CONFIRM	Ask the sender if they are sure they want to send the web message they entered.

SEND_FORMNAME	Allows specifying the form name in http posts and gets.
SEND_IDNAME	Allows specifying the idname text (id-name=recipient).
SEND_MSGNAME	Allows specifying the msgname text (msg-name=message).
SEND_SUCCESS	Specifies text in replys to posts that indicates success.
SEND_EXTRA	Specifies extra data that is posted after the message.

3.4.17   [idblock]

The idblock section is different from most of the ini settings. This section specifies multiple values per line. The line format is:

```
name|enabled|startid|endid|maxlen|sendfields|notification|backupnotification
```

Name is a descriptive name for this ID block.

Enabled may be set to N (or 0) to disable this range, or Y (or 1) to enable the range.

The startid is the first number of a number range to allow for this route. The endid is the ending number. If two ID blocks overlap the block with the smaller range will be used. To aid in readability dashes may be used to separate the number. For example, 843-555-0000 or 843-555-9999.

The maxlen parameter specifies the maximum length of the outgoing message. If the incoming message is longer than this it will be truncated.

Sendfields specifies which fields of an incoming email to send.

Notification and Backup Notification describe how the outgoing message will be sent. They are in the format of:

```
destination:idformat
```

where destination is the destination number of one of the destination profiles and idformat describes how the id is to be formatted. The idformat allows certain formatting variables to specify how the incoming pager ID is formatted for output.

For example, if your TAP output expects 7 digits, use %7i. The caller can send 7 or more digits in the ID and this will take the last 7 digits of the id for the output. If your callers typically send 7 digits and your paging terminal expects 10 digits you may prefix a number. For example, to prefix 843 use 843%7i. The 7 used in these examples can be other values. Some additional typical values are 4, 5, or 10.

The backup notification allows the message to be sent to another destination if the primary is down.

3.4.18   [modem]

Settings for various modems that may be used on the system. This section specifies multiple values per line. The line format is:

```
name|init1|init2|skipreset|hangupmethod|waitprotocol|answertimeout
```

Name is a descriptive name for this modem type and must begin with in-, out-, or em-. This specifies if the modem is used for inbound, outbound, or emulated.

Init1 and Init2 are init strings that are sent to the modem on startup. These are sent sequentially and an OK is expected back from the modem.

Skipreset allows overriding the default of a modem reset between calls.

Hangupmethod specifies how to force a modem to drop and hang-up a call. A 0 value uses DTR drop, a 1 value uses the "+++ATH" method.

Waitprotocol is set to 1 or Y to allow for modems that send a CONNECT string followed by a PROTOCOL string.

Answertimeout specifies the time to wait for a CONNECT from the modem.

3.4.19   [monitor]

This section controls the network monitor thread. This is where you will enter the
IP address and the interval to ping. You may also specify the number of tries before
considering the connection failed.

DEBUG_LEVEL	Level of debugging information to write to the debug directory. See the [common] section for a description of the values.
PING_INTERVAL	Specify the amount of time in seconds between pings.
PING_TRIES	Specify the number of failures before the connection is considered down.
PING_ADDRESS	Specify the IP address for the pings.
TEST_INTERVAL	This specifies how often to send the sequential tnpp test message in seconds. To disable this feature, set to 0.
TEST_DEVICE	This specifies the device name used to send the test page. To disable this feature, leave blank.
TEST_NOTIFICATION	If populated, this notification string will be used to send the sequential page, overriding the fields below.
TEST_CAPCODE	The capcode to receive the sequential page.
TEST_TNPPDEST	The destination tnpp node for the sequential page.
TEST_PAGERTYPE	The tnpp pager type for the sequential page.
TEST_PAGERCLASS	The tnpp pager class for the sequential page.
TEST_RFCHAN	the RF channel for the sequential page.
TEST_RFZONE	the RF zone for the sequential page.

ALLOW_MISSES	The number of sequential pages that can be missed without setting an alarm condition.
INTERVAL_ALLOWANCE	Value in seconds to allow sequential pages to be received.
RETRY_INTERVAL	Interval to use to resend a sequential page if it is not received.
ALARM_FROM	Name to use as the sender of alarm emails.
ALARM_TO	Name to use as the receiver of alarm emails.
ALARM_SUBJECT	Subject to use in alarm emails.
WATCHDOG_FROM	Name to use as the sender of watchdog emails. These go out at regular intervals for monitoring the IPT for proper operation.
WATCHDOG_TO	Name to use as the receiver of watchdor emails.
WATCHDOG_SUBJECT	Subject to use in watchdog emails.
WATCHDOG_INTERVAL	How often in seconds that watchdog emails are sent.
WALLUNIT_TIMECC	The capcode used to set the time in wallunits.
WALLUNIT_TIMEINTERVAL	How often the time is sent out to wallunits in seconds.
TAP_ALARM	The TAP id used to recieve periodic alarms.
TAP_INTERVAL	How often to send out tap alarms in seconds.

3.4.20   [passd]

ISI passthrough server.

DEBUG_LEVEL	Level of debugging information to write to the debug directory. See the [common] section for a description of the values.
BUFFER_SIZE	Specifies the size of the read buffer. This value will be used if one is not specified in the service table for the device. Shortcuts are allowed, so 65536 can also be entered as 64k.
READ_TIMEOUT	Specifies the initial and secondary read timeouts. The default value is 500:500. This is for a .5 second initial read timeout and a .5 second secondary read timeout. The initial read timeout is the amount of time in milliseconds the system waits for data. Once the system starts receiving data the secondary read timeout is used to wait for any additional data.
DEFAULT_PROFILE	The default passthrough profile to use if one is not specified in the port definition.

3.4.21   [passprofile]

Settings for the passthrough protocol. This section specifies multiple values per line. The line format is:

```
number|name|option|buffsize|inittime|sectime|linkinterval|linktries
```

Number is the profile number to use in the port definition.

Name is a description for the profile.

Option specifies the protocol options for this profile.

Buffsize specifies the size of the read buffer. Shortcuts are allowed, so 65536 can also be entered as 64k.

Inittime and Sectime specify the initial and secondary read timeouts. The default value is 10000 and 1000. This is for a 10 second initial read timeout and a 1 second secondary read timeout. The initial read timeout is the amount of time in milliseconds the system waits for data. Once the system starts receiving data the secondary read timeout is used to wait for any additional data.

LinkInterval is the time in seconds between sending <CR>'s and waiting for a '*' response.

LinkTries is the number of <CR>'s to send attempting to establish a link.

3.4.22   [rtview]

Real-time statistics viewer.

SCAN_TIME	The amount of time in milliseconds between screen refreshes in the rtview program. This value is typically 1000. Setting to 500 will set the refresh rate to 1/2 second. Values less than 200 are not recommended.
VERBOSE_LEVEL	Set to 1 to show ports which are currently not active, but have processed a connection previously. Set to 2 to show all ports whether or not they have had any activity.

3.4.23   [smppd]

SMPP server.

DEBUG_LEVEL	Level of debugging information to write to the debug directory. See the [common] section for a description of the values.
LISTEN_PORT	Specify the port used for internal SMPP packet forwarding. This port must not be used for any other service. Typically this is set to 1252.
MAX_QUEUE_ENTRIES	Number of queue entries to allocate for this protocol.
BUFFER_SIZE	Specifies the size of the read buffer. This value will be used if one is not specified in the service table for the device. Shortcuts are allowed, so 16384 can also be entered as 16k.

READ_TIMEOUT — Specifies the initial and secondary read timeouts. The default value is 30000:1000. This is for a 30 second initial read timeout and a 1 second secondary read timeout. The initial read timeout is the amount of time in milliseconds the system waits for data. Once the system starts receiving data the secondary read timeout is used to wait for any additional data.

INPUT_RATE — Specifies a time to delay sending a response to incomming messages to limit the input rate. The value of the delay is calculated in miliseconds as 60000/INPUT_RATE, for a range of 0 to 60000 ms (60 second). For no delay, enter 0.

OUTPUT_RATE — Specifies a delay between sending messages to limit the output rate. The value of the delay is calculated in miliseconds as 60000/INPUT_RATE, for a range of 0 to 60000 ms (60 second). For no delay, enter 0.

3.4.24 [smtpd]

SMTP server.

DEBUG_LEVEL — Level of debugging information to write to the debug directory. See the [common] section for a description of the values.

BUFFER_SIZE — Specifies the size of the read buffer. This value will be used if one is not specified in the service table for the device. Shortcuts are allowed, so 16384 can also be entered as 16k.

LISTEN_PORT — Specifies the port on which to listen. This is a TCP port from 1 to 65535. SMTP typically uses port 25. If 0 is used the port will be disabled.

PROTOCOL_OPTION — Specifies the protocol options specific to this protocol.

READ_TIMEOUT	Specifies the initial and secondary read timeouts. The default value is 30000:2000. This is for a 30 second initial read timeout and a 2 second secondary read timeout. The initial read timeout is the amount of time in milliseconds the system waits for data. Once the system starts receiving data the secondary read timeout is used to wait for any additional data.
IP_ALLOW	A list or range of IP addresses that are allowed to connect and send to us. Leave empty or 0.0.0.0 to allow all connections.
MAX_RECIPIENTS	Limits the number of recipients for each message. The value range is from 1 to 50.
MAX_EMAIL_LENGTH	Specifies the maximum size of the email in bytes.
SPAM_HEADER	Define the email header to look for for a floating point spam score. This field is used in combination with SPAM_SCORE to define the minimum value before a message is considered spam. This may also be used at the same time as SPAM_BOOLHEADER which specifies a header that contains a true/false value for spam.
SPAM_SCORE	The minimum score value that an incoming email can have before it is considered spam. This is a floating point value. For example, if this field is set to 3.1 an incoming email with a spam score of 3.1 or higher will be considered spam.
SPAM_ACTION	Defines what to do if an incoming email is considered spam. A value of 0, NONE, or ACCEPT will accept the email no matter what the spam headers are. 1 or REJECT will send back a reject message. 2 or DISCARD will just drop the incoming email. DISCARD is the recommended action.

SPAM_BOOLHEADER   Specifies the email header to look for a true/false indication that the message is spam. If the value in this header begins with an uppercase or lowercase Y or it is a greater than 0 numeric value the message will be considered spam. If this header doesn't exist in the incoming email the message will be accepted as non-spam.

FORWARDED_FOR_HEADER

specifies the header in the email which contains the original sender's IP address. This is used for matching in the emailfilt rules.

CHECK_DNSBL   Set to Y (or 1) to enable checking incoming connections against the list of dnsbl entries in the [dnsbl] section of ipt.ini.

THROTTLE_CODE   Specifies the error code sent when throttle limit is exceeded. The default value is 451. Valid range is from 400 to 599.

INPUT_RATE   Specifies a time to delay sending a response to incomming messages to limit the input rate. The value of the delay is calculated in miliseconds as 60000/INPUT_RATE, for a range of 0 to 60000 ms (60 second). For no delay, enter 0.

3.4.25   [snppd]

SNPP server.

DEBUG_LEVEL   Level of debugging information to write to the debug directory. See the [common] section for a description of the values.

BUFFER_SIZE   Specifies the size of the read buffer. This value will be used if one is not specified in the service table for the device. Shortcuts are allowed, so 16384 can also be entered as 16k.

LISTEN_PORT	Specifies the port on which to listen. This is a TCP port from 1 to 65535. SNPP typically uses port 444. If 0 is used the port will be disabled.
PROTOCOL_OPTION	Specifies the protocol options specific to this protocol.
READ_TIMEOUT	Specifies the initial and secondary read timeouts. The default value is 30000:1000. This is for a 30 second initial read timeout and a 1 second secondary read timeout. The initial read timeout is the amount of time in milliseconds the system waits for data. Once the system starts receiving data the secondary read timeout is used to wait for any additional data.
IP_ALLOW	A list or range of IP addresses that are allowed to connect and send to us. Leave empty or 0.0.0.0 to allow all connections.
MAX_RECIPIENTS	Limits the number of recipients for each message. The value range is from 1 to 50.
INPUT_RATE	Specifies a time to delay sending a response to incomming messages to limit the input rate. The value of the delay is calculated in miliseconds as 60000/INPUT_RATE, for a range of 0 to 60000 ms (60 second). For no delay, enter 0.
MAX_CONNTIME	Maximum time in minutes a single connection is allowed.

3.4.26   [tapd]

TAP server.

DEBUG_LEVEL	Level of debugging information to write to the debug directory. See the [common] section for a description of the values.
LISTEN_PORT	Specifies the port on which to listen. This is a TCP port from 1 to 65535. If 0 is used the port will be disabled.

MAX_QUEUE_ENTRIES	Number of queue entries to allocate for this protocol.
BUFFER_SIZE	Specifies the size of the read buffer. This value will be used if one is not specified in the service table for the device. Shortcuts are allowed, so 16384 can also be entered as 16k.
READ_TIMEOUT	Specifies the initial and secondary read timeouts. The default value is 30000:1000. This is for a 30 second initial read timeout and a 1 second secondary read timeout. The initial read timeout is the amount of time in milliseconds the system waits for data. Once the system starts receiving data the secondary read timeout is used to wait for any additional data.
IP_ALLOW	A list or range of IP addresses that are allowed to connect and send to us. Leave empty or 0.0.0.0 to allow all connections.
DEFAULT_PROFILE	The default tap profile to use if one is not specified in the port definition.
INPUT_RATE	Specifies a time to delay sending a response to incomming messages to limit the input rate. The value of the delay is calculated in miliseconds as 60000/INPUT_RATE, for a range of 0 to 60000 ms (60 second). For no delay, enter 0.

3.4.27   [tapprofile]

Settings for the TAP protocol. This section specifies multiple values per line. The line format is:

```
number|name|option|t1|t2|t3|t4|t5|n1|n2|n3
```

Number is the profile number to use in the port definition.

Name is a description for the profile.

Option specifies the protocol options for this profile.

T1 is the <CR> repeat rate waiting on ID= (client default = 2000).

T2 is the time after <CR> seen to sent ID= (server default = 1000).

T3 is the time to wait for a response to a packet (client default = 10000).

T4 is the time to wait for another packet (server default = 4000).

T5 is the time to wait for response to ID= (server default = 8000).

N1 is the number if <CR>'s to send while looking for ID= (client default = 3).

N2 is the number of times a packet can be resent if <NAK> is seen (client default = 3).

N3 is the number of ID='s that can be sent (server default = 3).

3.4.28   [tnppd]

TNPP server.

DEBUG_LEVEL	Level of debugging information to write to the debug directory. See the [common] section for a description of the values.
LISTEN_PORT	Specify the port used for internal TNPP packet forwarding. This port must not be used for any other service. Typically this is set to 1251.
MAX_QUEUE_ENTRIES	Number of queue entries to allocate for this protocol.
BUFFER_SIZE	Specifies the size of the read buffer. This value will be used if one is not specified in the service table for the device. Shortcuts are allowed, so 16384 can also be entered as 16k.
READ_TIMEOUT	Specifies the initial and secondary read timeouts. The default value is 30000:1000. This is for a 30 second initial read timeout and a 1 second secondary read timeout. The initial read timeout is the amount of time in milliseconds the system waits for data. Once the system starts receiving data the secondary read timeout is used to wait for any additional data.
IP_ALLOW	A list or range of IP addresses that are allowed to connect and send to us. Leave empty or 0.0.0.0 to allow all connections.
DEFAULT_PROFILE	The default tnpp profile to use if one is not specified in the port definition.
INPUT_RATE	Specifies a time to delay sending a response to incomming messages to limit the input rate. The value of the delay is calculated in miliseconds as 60000/INPUT_RATE, for a range of 0 to 60000 ms (60 second). For no delay, enter 0.
SOURCE_ID	The source id that is used for this tnpp node. Used when sending init packets and when creating tnpp packets to be sent.

3.4.29   [tnppprofile]

Settings for the TNPP protocol. This section specifies multiple values per line. The line format is:

```
number|name|option|tict|tnri|tnre|thold|tidle|cenqmax|choldmax|
cretrymax|simplextransmits
```

Number is the profile number to use in the port definition.

Name is a description for the profile.

Option specifies the protocol options for this profile. Option bit 0 if set turns on transparent CRC, Option bit 1 if set specifies a simplex link, Option bit 15 if set specifies multicast.

Tict, Tnri, Tnre, Thold, Tidle, Cenqmax, Choldmax, and Cretrymax are timers and counts defined by the TNPP protocol specification.

Simplextransmits specifies the number of times to repeat a tnpp simplex packet.

3.4.30   [tnpproute]

Settings for the TNPP routing. This section specifies multiple values per line. The line format is:

```
dest|name|enabled|device
```

dest

Specifies an entry for a TNPP destination node. Multiple entries supported per destination node.

name

a discriptive name for a route entry.

enabled

set to 'Y', 'y' or non-zero to enable this entry.

device

specifies the output for this route. If the output is serial, then this must have a port entry with a matching DEVICE_NAME (ie. /dev/ttyUSB0). If the output is network based, than use the format host:port. As of kernel builds on or after Oct 1, 2012 tcp/ip multicast is supported. (ie. 224.1.1.1:777).

3.4.31   [port...]

Port settings. A port is typically an RS-232 port or a modem, but may be a persistent network connection to a remote server.

DEVICE_NAME   This is the device name associated with the port.
                   The device could be in /dev, a COM, or network
                   device. If the name does not begin with /dev or
                   COM, than it is assumed to be a network address
                   or domain name.

ENABLED   If this value is '1', 'Y' or 'y', then the port is
                   opened automatically at startup. Values of '0',
                   'N', or 'n' disable.

ALLOW_IDBLOCK   Allows idblock lookups on incoming traffic.

DESC   Allows a descriptive name to be associated with
                   the port.

DEBUG_LEVEL   Level of debugging information to write to the de-
                   bug directory. See the [common] section for a de-
                   scription of the values.

TNPP_ID   The tnpp source ID associated with this port.

PROTOCOL   The protocol used to communicate on this port.
                   Valid values are one of: DECODER, ENCODER,
                   GCP, PASS, ISI, SMPP, SMS, TAP, TNPP,
                   HEARTBEAT, VMODEM.

DIRECTION   Indicates if the port is an input, output, or both.
                   Use '1' or 'IN' for input, '2' or 'OUT' for output,
                   '3' or 'BOTH' for both.

MAX_MSGLEN   Specifies the maximum message length. Longer
                   messages are truncated. Keep in mind other
                   MAX_MSGLEN values may also impact traffic on
                   this port. This value can be from 1 to 990.

PROFILE   This specifies which protocol profile line to use to
                   get options and parameters.

NOTIFICATION   Allows overriding the ID_BLOCK and SUB-
                   SCRIBER notification settings for this port.

BACKUP_NOTIFICATION	Allows overriding the ID_BLOCK and SUB-SCRIBER backup notification settings for this port.
INPUT_RATE	Specifies a time to delay sending a response to incomming messages to limit the input rate. The value of the delay is calculated in miliseconds as 60000/INPUT_RATE, for a range of 0 to 60000 ms (60 second). For no delay, enter 0.
OUTPUT_RATE	Specifies a delay between sending messages to limit the output rate. The value of the delay is calculated in miliseconds as 60000/INPUT_RATE, for a range of 0 to 60000 ms (60 second). For no delay, enter 0.
LOG_TYPE	Specifies the logging type for the port. No value, 'OFF', 'NONE', and '0' disable logging. A value of 'IN' or '1' log input traffic. A value of 'OUT' or '2' log output traffic. A value of 'BOTH' or '3' logs both directions.
HOST	Specifies the IP address of the host port that the client will connect to.
PORT	Specifies the port to connect to, or listen on. The value must be between 0 and 65535.
SOCK_DOMAIN	This defines the type of connection and defaults to 2 for INET, used in most cases. If a UNIX domain is required, enter 1 for 'UNIX'.
SOCK_TYPE	Defines the sock type. The default is 1 for SOCK_STREAM. Enter 1 for standard TCP, or 2 for SOCK_DGRAM or UDP.
SOCK_ADDR	Defines the IP address or domain name to connect to.
SOCK_PORT	Defines the TCP port to connect or listen on. The value can be from 0 to 65535.

USERNAME	Defines the username for logon, if required by the host.
PASSWORD	Defines the password for logon, if required by the host.
SYSTEM_TYPE	Defines the SMPP system type, if required.
MODEM_TYPE	Defines which modem_profile to use.
BAUD	Specifies the baudrate. Maximum is 115200 (except for encoder).
PARITY	Specifies the parity, enter E for Even or N for no parity.
DATABITS	Specifies the number of bits used to transmit data. Enter values of 7 or 8.
STOPBITS	Specifies the number of stopbits. Enter a value of 1 or 2.
FREQUENCY	Specifies the RF Frequency to monitor. Used only if protocol is DECODER.
MAX_QUEUE_ENTRIES	Specifies the number of que entries to allocate for this port.
PING_INTERVAL	Specifies the ping interval used by the ENCODER and HEARTBEAT protocols.
ZONE_PROFILE	Specifies the zone profile to use when protocol is ENCODER.
CHANNEL	Specifies the channel number when protocol is ENCODER.

3.4.32   subaccess

The subaccess table defines passwords and access levels. This is primarily used to provide login control for HTTP, SNPP, and WCTP.

Fields

username	The login username. This value may be up to 16 characters long.
password	The login password. This value may be up to 16 characters long.
enabled	This is set to 1 to enable the login. Set to 0 to temporarily disable this login.
realname	The real name for the login. This is a descriptive name and can be the user's full name. This value may be up to 32 characters long.
accesslevel	The subscriber access level. Currently only the value of 1 is supported to allow paging via SNPP and WCTP. If this field is set to 0 the login will not be allowed to send messages via SNPP or WCTP.
pagemask	Sets a mask of bits that allows this login to be able to page certain subscribers. See subscriber.pagemask also. This field should be set to 0xffffffff to be able to page any subscriber in the system. If you want to only allow this login to be able to page certain subscribers the pagemask in subscriber will be logically ANDed with this value and if the result is non-zero the access is allowed. For example, if the subscriber pagemask is 0x00000001 and the subaccess pagemask is 0x00000002 the access isn't allowed.
badloginattempts	The number of bad login attempts for this subscriber. This should normally be zero unless someone has used the wrong password to login. If the user is locked out due to too many bad login attempts, set this to 0 to allow them to login again.
maxloginattempts	The maximum number of bad login attempts before the username is locked. Once a username is locked you will need to manually set the badloginattempts to 0 so they can login again.

sourceaddress	The source address to use for outgoing SMPP connections. By using this with an SNPP login you can override the default SMPP source address with this value.
enabletracking	Not currently used.
allowcommand	Not currently used.

3.4.33   [subscriber]

The subscriber table contains the subscriber information for accepting incoming messages.

Fields

subscriberid	The unique subscriber identifier. Usually their 7 or 10-digit pager number. This value may be up to 16 characters long.
enabled	Set to 0 to temporarily disable the subscriber. For example temporarily invalidating a pager due to non-payment.
showinlist	Controls whether or not the subscriber is shown on the drop-down list on the web paging form.
listorder	The order in the drop down web paging list. Subscribers with the same listorder number will be in subscriberid order.
description	Descriptive name.
accountnumber	The subscriber's account number. This is an information only field and does not affect the operation of the IPT.
passcode	The subscriber passcode. This value may be up to 8 characters long. This is not currently used and is reserved for future use.

callerpasscode   The caller passcode. This value may be up to 8
                                characters long. This is used to restrict incom-
                                ing messages to callers that know the subscriber's
                                caller passcode.

answertype   Used for DID modem to control whether the in-
                                coming call send DTMF digits for numeric paging
                                or the DID modem answers and accepts TAP mes-
                                sages. For all other uses this field is ignored and
                                can be set to 0. To answer a DID input with mo-
                                dem tones for accepting a TAP call set this field
                                to 1. Otherwise, to accept a DTMF numeric page
                                via the DID input set this field to 0.

allowsource   Specify with which protocols the subscriber is al-
                                lowed to receive messages. The following is a list.
                                Multiple values can be ANDed (added) together.

Source	Value	Description
GCP	0x00000001	Glenayre Computer Protocol
HTTP	0x00000002	Hyper Text Tranfer Protocol
SMPP	0x00000004	Short Message Peer to Peer
SMTP	0x00000008	Simple Mail Transfer Protocol
SNPP	0x00000010	Simple Network Paging Protocol
TAP	0x00000020	Telecator Alphanumeric Protocol
TNPP	0x00000040	Telecator Network Paging Protocol
WCTP	0x00000080	Wireless Communications Transfer Protocol

pagemask   Only allow certain subaccess logins the ability to
                                page this subscriber. Set this to 0 to allow all
                                subaccess logins to page this subscriber. Other-
                                wise the subaccess pagemask will be ANDed with
                                this to control messages to this subscriber.

maxmessagelen   The maximum message length the subscriber is
                                allowed to receive. The default value is 240. Al-
                                lowable values are from 1 to 990.

sendfields   Specifies which fields of an incoming email to send.
                                This is a string field that accepts F, S, and B.
                                F=from, S=subject, and B=body. Combinations
                                are supported (e.g. FSB or SB).

replyto	Set the reply to email address for outgoing emails.

3.4.34 [pager]

The pager table contains the outgoing notification information for the individual subscribers.

Fields

subscriberid	The unique subscriber identifier. This must be set to a subscriberid that exists in the subscriber table.
sequence	A unique sequence number for this pager record. Multiple pagers per subscriber are supported. Increment this number for each subscriber. This does not need to be unique across all subscribers. For example, both subscriber 1234 can have a sequence 1 and subscriber 1235 can have a sequence 1.
enabled	This is set to 1 to allow the message to be sent to this pager record. Set to 0 to temporarily disable this notification device.
notification	Primary notification device. This is in the form of destprofile:recipient. Some recipients are straightforward like an email recipient of pager@example.com. Others are more complex like the encoder which uses a format of capcode:format:class:function:priority. You may also use an ID format like %10i to send the 10-digit ID.

backupnotification   Backup notification device. This is specified us-
                                   ing the same format as notification above. This is
                                   used if the message can not be sent to the notifi-
                                   cation device.

3.5   Example ipt.ini

```
[common]
DEBUG_LEVEL=0x0000ffff
MASQUERADE_AS=
HELO_NAME=
ERROR_HOST=:0
DEBUG_HOST=:0
LOG_HOST=:0
RLIMIT_MSGQUEUE=16777216
THREAD_STACK_SIZE=262144
SMART_HOST=:0
SMARTHOST_TIMEOUT=0
EMAIL_FROM=
EMAIL_SUBJECT=
EMAIL_FORMAT=0
EMAIL_PREFIX_FROM=Fr:
EMAIL_PREFIX_TO=To:
EMAIL_PREFIX_SUBJECT=Su:
EMAIL_PREFIX_BODY=Msg:
RETRY_MAX_RETRIES=2
RETRY_INTERVAL=1
DEFAULT_THROTTLE=1
MAX_FROM_LENGTH=16
MAX_SUBJECT_LENGTH=80
MAX_MESSAGE_LENGTH=990
ALLOW_DOMAINS=harktech.com,pager.harktech.com,ipt.harktech.com
IP_ALLOW=0.0.0.0
PURGE_DEBUG_DAYS=1
PURGE_DEBUG_HOUR=1
STRIP_PLUSONE=N
RANDOM_DEVICE=PRNG
BROADCAST_SEND=N
SYSTEM_IDENTIFIER=Hark Technologies
TUNNEL_USER=0050c2b96126
TUNNEL_PORT=50294

[ethernet]
PRIMARY_MODE=DHCP
PRIMARY_MAC=00:50:C2:B9:61:26
PRIMARY_HOSTNAME=ipt.harktech.com
PRIMARY_IP=
PRIMARY_NETMASK=
PRIMARY_ETH1_MODE=DISABLED
PRIMARY_ETH1_MAC=
PRIMARY_ETH1_IP=
```

```
PRIMARY_ETH1_NETMASK=
STANDBY_MODE=DISABLED
STANDBY_MAC=
STANDBY_HOSTNAME=
STANDBY_IP=
STANDBY_NETMASK=
STANDBY_ETH1_MODE=DISABLED
STANDBY_ETH1_MAC=
STANDBY_ETH1_IP=
STANDBY_ETH1_NETMASK=
VIRTUAL_IP=
VIRTUAL_NETMASK=
GATEWAY=
NAMESERVER1=
NAMESERVER2=

[encoderprofile]
#number|name|option|stationid|idinterval|idtonedelta|keyupdelay|keydowndelay|
#maxkeytime|maxpacket|watchdog|mtonehi|mtonelo|mhilo|datainvert|
#digitalid|prebits|pretonegap|pretonetime|pretonefreq|voicealerttime|
#cor|idlekey|latency|atcbatchgap
1|Default|0x00000000|HARKIPT|900|1800|200|300|0|1024|0|2200|1200|N|Y|2|100|500|250|1000|2000|0|
2|atc|0xc00000ff|HARKATC|0|1800|200|0|0|1024|0|2200|1200|N|Y|2|100|500|250|1000|2000|0|0|3000|2

[fivetoneprofile]
#number|name|timeout|waketime|wakegap|pretime|pregap|tonetime|idtgap|functime|
#pagegap|spclrepeat
1|Default|5|690|45|690|45|33|0|52|52|N

[golayprofile]
#number|name|timeout|invert
1|Default|5|N

[pocsagprofile]
#number|name|timeout|512xtracomma|1200xtracomma|2400xtracomma|pad|invert
1|Default|5|0|0|0|0|N

[ravenprofile]
#number|name|timeout|512xtracomma|1200xtracomma|commabytes
1|Default|1|0|0|650

[twotoneprofile]
#number|name|timeout|gap|gaptime|pagegap|atime|btime|grouptime|groupextra
1|Default|5|N|200|250|1000|3000|8000|1700

[zoneprofile]
#number|name|analogkey|digitalkey|guardtone|gtonedelta|purc
1|Default|1|3|2|2175|2175:120,1950:40

[destprofile]
#serial format
#num|name|en|1|prot|option|comport|idfmt|maxlen|tries|mdmtype|mdmnum|baud|par|data|stop
#network format
#num|name|en|2|prot|option|host|port|idformat|maxlen|tries|username|password|connecttimeout
#ENCODER adds channel|zone|tnppdest|inertia to end
```

```
#SMS adds sourceaddr to end
#TAP adds tappassword to end
#TNPP adds tnppdest|channel|zone|inertia to end
1|encoder|Y|1|ENCODER|0|/dev/ttyUSB6|%10i|240|1|||460800|N|8|1|8|1|0|0
2|atc|Y|1|ENCODER|0xc00000ff|/dev/null|%10i|4800|1|||38400|N|8|1|1|1|0001|3
10|HARK SNPP|Y|2|SNPP|0|c5nms.harktech.com|444|%10i|240|1|||2000
40|TAP out|Y|1|TAP|0|/dev/ttyUSB0|%7i|240|1|||9600|E|7|1|000000
50|TNPP out|Y|1|TNPP|0|/dev/ttyUSB0|%7i|240|1|||9600|N|8|1|0001|0|0|3
60|SMS out|Y|1|SMS|0|/dev/ttyUSB4|%10i|160|1|||9600|N|8|1|8432199019
100|Dial Backup|Y|1|TAP|0|/dev/ttyUSB4|%7i|240|1|out-mt|102|115200|E|7|1|

[dnsbl]
bl.spamcop.net|1|mail rejected; see http://www.spamcop.net
sbl-xbl.spamhaus.org|1|mail rejected; see http://www.spamhaus.org

[gcpprofile]
#number|name|option|buffsize|inittime|sectime|linkinterval|linktries
# option 0x08000000=requirelogin
1|default|0|1024|10000|1000|10|3

[gcpd]
DEBUG_LEVEL=0x0000ffff
LISTEN_PORT=3021
MAX_QUEUE_ENTRIES=16
IP_ALLOW=
DEFAULT_PROFILE=1
VERSION=6.100

[heartbeat]
PING_INTERVAL=30
PING_ADDRESS=10.100.1.254
PING_TIMEOUT=100
PING_TRIES=0

[httpd]
DEBUG_LEVEL=0x0000ffff
LISTEN_PORT=80
PROTOCOL_OPTION=0x00000000
BUFFER_SIZE=65536
READ_TIMEOUT=30000:1000
IP_ALLOW=
SESSION_EXPIRE=2880
SHOW_SUBLIST=N
SHOW_FROM=Y
SHOW_SUBJECT=Y
SHOW_CONFIRM=N

[idblock]
#name|enabled|start|end|max_msglen|sendfields|notification|backupnotification
default|Y|0|9999999999|240|FSB|10:%10i|

[modem]
#name|init1|init2|skipreset|hangupmethod|waitprotocol|answertimeout
out-usr|AT&FE|AT&H0&I0&K0&M0&R1S7=45S10=1S12=0&W|0|0|0|0
out-usrhs|AT&FE|ATE0&C1&D2&W|0|0|0|0
```

```
out-cell|||1|0|0|45000
out-mt|AT&FE|ATX1&K0&Q6%C0&W|1|0|0|45000
out-mths|AT&FE|AT&W|1|0|0|45000
out-uds24|AT&FE|ATE0&C1&D2%K0S7=30&W|0|0|0|0
out-uds96|AT&FE|ATE0&C1&D2%B0%C0\N0\Q0S7=30&W|0|0|0|0
out-xecom92|AT&H4%C0\N0||1|1|0|0
out-xecom24|ATE0\N0||1|1|0|0
em-modem|||1|0|0|0
in-did|ATDBG=0|ATCFG=7,5000,3000,250,500,500,2000,4000,10,y|1|0|0|45000
in-mtvoice|AT&FE|AT&W|1|0|0|10000
in-mt|AT&FE\V1+MS=V22B,1,300,2400,300,2400|ATS0=1&W|1|0|0|45000

[monitor]
DEBUG_LEVEL=0x0000ffff
PING_INTERVAL=0
PING_TRIES=2
PING_ADDRESS=
TEST_INTERVAL=0
TEST_DEVICE=
TEST_NOTIFICATION=
TEST_CAPCODE=
TEST_TNPPDEST=
TEST_PAGERTYPE=
TEST_PAGERCLASS=
TEST_RFCHAN=0
TEST_RFZONE=0
ALLOW_MISSES=0
INTERVAL_ALLOWANCE=0
RETRY_INTERVAL=0
ALARM_FROM=
ALARM_TO=
ALARM_SUBJECT=
WATCHDOG_FROM=
WATCHDOG_TO=
WATCHDOG_SUBJECT=
WATCHDOG_INTERVAL=0
WALLUNIT_TIMECC=
WALLUNIT_TIMEINTERVAL=0
TAP_ALARM=
TAP_INTERVAL=0

[passprofile]
#number|name|option|buffsize|inittime|sectime|linkinterval|linktries
# option 0x02=ISI linktest
1|default|0|1024|200|200|60|3

[passd]
DEBUG_LEVEL=0x0000ffff
BUFFER_SIZE=2048
READ_TIMEOUT=500:500
DEFAULT_PROFILE=1

[rtview]
SCAN_TIME=500
VERBOSE_LEVEL=2
```

```
[smppd]
DEBUG_LEVEL=0x0000ffff
LISTEN_PORT=2775
MAX_QUEUE_ENTRIES=10
BUFFER_SIZE=1024
READ_TIMEOUT=30000:1000
INPUT_RATE=60
OUTPUT_RATE=60

[smsd]
DEBUG_LEVEL=0x0000ffff
MAX_QUEUE_ENTRIES=10
BUFFER_SIZE=1024
READ_TIMEOUT=30000:1000

[smtpd]
DEBUG_LEVEL=0x0000ffff
LISTEN_PORT=25
BUFFER_SIZE=16384
PROTOCOL_OPTION=0x00000000
READ_TIMEOUT=30000:2000
IP_ALLOW=
MAX_RECIPIENTS=10
MAX_EMAIL_LENGTH=100000
SPAM_HEADER=X-Spam-Score
SPAM_SCORE=0.000
SPAM_ACTION=2
SPAM_BOOLHEADER=X-Spam-Flag
CHECK_DNSBL=Y
FORWARDED_FOR_HEADER=X-Forwarded-For
THROTTLE_CODE=451
INPUT_RATE=60

[snppd]
DEBUG_LEVEL=0x0000ffff
LISTEN_PORT=444
BUFFER_SIZE=1024
PROTOCOL_OPTION=0x00000000
READ_TIMEOUT=30000:1000
IP_ALLOW=
MAX_RECIPIENTS=10
INPUT_RATE=60
MAX_CONNTIME=1

[tapprofile]
#number|name|option|t1|t2|t3|t4|t5|n1|n2|n3|autolimit|manuallimit
# option 0x01=transchar, 0x02=extblock, 0x04=norespcode, 0x04000000=netevenparity
1|default|0|2000|1000|10000|4000|8000|3|3|3

[tapd]
DEBUG_LEVEL=0x0000ffff
LISTEN_PORT=8273
MAX_QUEUE_ENTRIES=32
BUFFER_SIZE=1024
```

```
READ_TIMEOUT=30000:1000
IP_ALLOW=
DEFAULT_PROFILE=1
INPUT_RATE=60

[tnppprofile]
#number|name|option|tict|tnri|tnre|thold|tidle|cenqmax|choldmax|cretrymax|simplextransmits
# option 0x01=transcrc, 0x02=simplex
1|default|0|2000|10000|10000|10000|60000|6|24|6|1

[tnpproute]
#dest|name|enabled|device
0001|serial|Y|/dev/ttyUSB0
0001|network|Y|224.1.1.1:777

[tnppd]
DEBUG_LEVEL=0x0000ffff
LISTEN_PORT=8677
MAX_QUEUE_ENTRIES=32
BUFFER_SIZE=4096
READ_TIMEOUT=30000:1000
DEFAULT_PROFILE=1
IP_ALLOW=
INPUT_RATE=60
SOURCE_ID=

[vmodem]
DEBUG_LEVEL=0xffffffff
PROTOCOL_OPTION=0x00000000
BUFFER_SIZE=16384
READ_TIMEOUT=10000:2000
MAX_RINGS=2
NUMBEEP_COUNT=3
NUMBEEP_FREQ=2000
NUMBEEP_ONTIME=200
NUMBEEP_OFFTIME=50

[port1]
DEVICE_NAME=/dev/ttyUSB0
ENABLED=Y
ALLOW_IDBLOCK=Y
DESC=test
DEBUG_LEVEL=0x0000ffff
PROTOCOL=PASS
DIRECTION=1
MAX_MSGLEN=240
PROFILE=1
INPUT_RATE=0
OUTPUT_RATE=0
LOG_TYPE=0
HOST=
PORT=10001
USERNAME=
PASSWORD=
MODEM_TYPE=NONE
```

```
BAUD=9600
PARITY=N
DATABITS=8
STOPBITS=1

[port2]
DEVICE_NAME=/dev/ttyUSB1
ENABLED=Y
ALLOW_IDBLOCK=Y
DESC=test
DEBUG_LEVEL=0x0000ffff
PROTOCOL=PASS
DIRECTION=1
MAX_MSGLEN=240
PROFILE=1
INPUT_RATE=0
OUTPUT_RATE=0
LOG_TYPE=0
HOST=
PORT=10002
USERNAME=
PASSWORD=
MODEM_TYPE=NONE
BAUD=9600
PARITY=N
DATABITS=8
STOPBITS=1

[port3]
DEVICE_NAME=/dev/ttyUSB2
ENABLED=Y
ALLOW_IDBLOCK=Y
DESC=test
DEBUG_LEVEL=0x0000ffff
PROTOCOL=PASS
DIRECTION=1
MAX_MSGLEN=240
PROFILE=1
INPUT_RATE=0
OUTPUT_RATE=0
LOG_TYPE=0
HOST=
PORT=10003
USERNAME=
PASSWORD=
MODEM_TYPE=NONE
BAUD=9600
PARITY=N
DATABITS=8
STOPBITS=1

[port4]
DEVICE_NAME=/dev/ttyUSB3
ENABLED=Y
ALLOW_IDBLOCK=Y
```

```
DESC=test
DEBUG_LEVEL=0x0000ffff
PROTOCOL=PASS
DIRECTION=1
MAX_MSGLEN=240
PROFILE=1
INPUT_RATE=0
OUTPUT_RATE=0
LOG_TYPE=0
HOST=
PORT=10004
USERNAME=
PASSWORD=
MODEM_TYPE=NONE
BAUD=9600
PARITY=N
DATABITS=8
STOPBITS=1

[port5]
DEVICE_NAME=/dev/ttyUSB4
ENABLED=n
ALLOW_IDBLOCK=N
DESC=test
DEBUG_LEVEL=0x0000ffff
PROTOCOL=TAP
DIRECTION=2
MAX_MSGLEN=240
PROFILE=1
INPUT_RATE=0
OUTPUT_RATE=0
LOG_TYPE=0
USERNAME=
PASSWORD=
MODEM_TYPE=out-mt
BAUD=115200
PARITY=E
DATABITS=7
STOPBITS=1

[subaccess]
#login|pass|enabled|realname|accesslevel|pagemask|badattempts|maxattempts|
#sourceaddress|enabletracking|allowcommand

[subscriber]
#subscriberid|enabled|showinlist|listorder|description|accountnumber|passcode|
#callerpass|answertype|allowsource|pagemask|maxmsglen|sendfields|replyto

[pager]
#subscriberid|sequence|enabled|notification|backupnotification

[canmsg]
#description|text

[watcher]
```

```
#filename|pin
```

Chapter 4

Program Descriptions

The following sections describe the executables that make up the IPT application. For Linux systems the base directory is /usr/local.

4.1 Introduction

4.2 System programs

These programs must always be running for the system to operate.

4.2.1 iptd

iptd is the master program that starts all of the protocol and maintenance threads.

4.3 Protocol servers

4.3.1 gcpd

This program allows incoming messages using the Glenayre Computer Protocol. This can be used to accept input from the Hark TAP-2000.

The Omega also supports a limited computer interface using GCP. The following commands are supported:

- @RV read version.

- @PO page out

The "read version" command above will return one of '6.000*', '6.100*', or '8.000*' based on the version set in the service record.

Verision 2.12 supports programming subscriber pager records with @CR, @MR, @DR, @RE.

Other commands will return ?02 Unknown command. The lower-case versions of these commands are also supported. For example, the @PO command takes a two-digit field number for the key (e.g. @PO#01/) and the @po command takes a three-digit field number for the key (e.g. @po#070/).

4.3.2   httpd

Accepts incoming HTTP requests. This is used for both subscriber web access and administrator web access. The httpd server supports template based web pages. The web pages are stored in /usr/local/www and may be customized based on your specific needs.

The web pages are standard HTML but have special tags for substitution and other uses. These tags are <@@ and @@> anything between these two tags are parsed by the web server and replaced with the proper value.

4.3.3   passd

Acts as a server for connecting remote serial ports over a network connection using Hark ISI devices. The remote serial ports can be transported over the internet and come out on a serial port on the Omega-LX for local access. The Omega-LX can also be configured as a capture device for remote logging. Set the protocol option to 1 to log all the data recived to a capture file for the current day in the capture directory. The capture directory is accessible through the web admin page.

4.3.4   smppd

A bi-directional SMPP server supporting SMPP v3.3 and SMPP v3.4. Messages longer than 160 (254 in SMPP v3.4) characters are supported using the message_payload TLV. The callback_num TLV is also supported when sending SMPP messages.

4.3.5 smtpd

Accepts incoming email messages and pages them out based on the subscriber ID.

If the message has attachments, they are automatically stripped. Only plain text portions of the email are sent to the pager.

4.3.6 snppd

Handles all incoming Internet Simple Network Paging Protocol messages. SNPP is described in RFC 1861 `http://www.faqs.org/rfcs/rfc1861.html`.

In the command list below only the capitalized letters are needed for the command. For example, MESS or MESSage will enter the message for the pager. Also, these commands are not case-sensitive, both MESS and mess will enter the message. See the RFC for more information.

The SNPP RFC does not mention a limit on the length of the incoming command. The IPT will accept up to 16384 bytes per line, but some SNPP servers may be limited to as little as 1024.

The IPT supports the following SNPP commands:

- PAGEr <pagerid>

- MESSage <message>

- RESEt

- SEND

- QUIT

- HELP

The following level 2 commands are supported:

- LOGIn <username> [password]

- PAGEr <pagerid> [passcode]

- DATA

- HOLD <YYMMDDhhmm> [+/- GMT difference]

- CALLerid <callerid>

- SUBJect <subject>

4.3.7   tapd

Handles all incoming TAP protocol connections. The TAP protocol is supported on direct RS-232 connections, modem connections, and TCP connections. In order to accept incoming TAP connections from the internet the Host field needs to be empty signifying a server connection.

The TAP protocol server now supports configurable timers as specified in TAP 1.8 Section 7.0 page 16. These are named t1 through t5 and n1 through n3. See the table below for description and default values:

Name	Default	Description
t1	2000	Repeat CR until ID= (client)
t2	1000	Time after CR to wait for ID= (client)
t3	10000	Time to wait for packet response (client)
t4	4000	Time to wait for incoming packet (server)
t5	8000	Time to wait for ID= (server)
n1	3	Number of CR to send looking for ID= (client)
n2	3	Number of packet resends (client)
n3	3	Number of ID= to send (server)

4.3.8   tnppd

Handles all incoming and outgoing TNPP protocol connections. Tnppd acts as a full TNPP router with packet remapping and filtering capabilities. The TNPP protocol is supported on direct RS-232 connections, modem connections, and TCP connections. Both client and server connections are supported.

4.3.9   wctpd

The WCTP server uses the URL of http://wctp.yourdomainname.com/wctp (replace yourdomainname.com with your internet domain name) to receive pages.

The following portions of the WCTP DTD are supported:

- wctp-Operation

  - wctpVersion
  - wctpToken

- wctp-ClientQuery

  - senderID
  - recipientID
  - trackingNumber

- wctp-ClientQueryResponse
  - minNextPollInterval
- wctp-ClientMessage
- wctp-ClientStatusInfo
- wctp-ClientResponseHeader
  - responseTimestamp
  - respondingToTimestamp
- wctp-Confirmation
- wctp-Success
  - successCode
  - successText
- wctp-MessageReply
- wctp-ResponseHeader
  - responseToMessageID
  - responseTimestamp
- wctp-PollForMessages
  - pollerID
  - securityCode
  - maxMessagesInBatch
- wctp-MessageReceived
  - sequenceNo
- wctp-PollResponse
  - minNextPollInterval
- wctp-Message
  - sequenceNo
- wctp-NoMessages
- wctp-Failure
  - errorCode
  - errorText

- wctp-Notification

  - type

- wctp-SubmitClientMessage

  - wctp-SubmitClientHeader

    * submitTimeStamp

  - wctp-ClientOriginator

    * senderID
    * miscInfo

  - wctp-ClientMessageControl

    * sendResponsesToID
    * allowResponse
    * notifyWhenQueued
    * notifyWhenDelivered
    * notifyWhenRead
    * deliveryAfter
    * preformatted
    * allowTruncation

  - wctp-Payload

    * wctp-Alphanumeric
    * wctp-TransparentData

- wctp-SubmitClientResponse

- wctp-ClientSuccess

  - successCode
  - successText
  - trackingNumber

- wctp-SubmitRequest

  - wctp-SubmitHeader

    * submitTimeStamp

  - wctp-Originator

    * senderID
    * securityCode

  - wctp-Recipient

    * recipientID
    * authorizationCode

- – wctp-MessageControl
    - ∗ messageID
    - ∗ sendResponsesToID
    - ∗ allowResponse
    - ∗ notifyWhenQueued
    - ∗ notifyWhenDelivered
    - ∗ notifyWhenRead
    - ∗ deliveryAfter
    - ∗ preformatted
    - ∗ allowTruncation
  - – wctp-Payload
    - ∗ wctp-Alphanumeric
    - ∗ wctp-TransparentData

- wctp-VersionQuery

  - – inquirer
  - – dateTime

- wctp-VersionResponse

  - – responder
  - – inquirer
  - – dateTimeOfReq

- wctp-ContactInfo

  - – email
  - – phone
  - – www
  - – info

- wctp-DTDSupport

  - – dtdName

4.4 Maintenance programs

4.4.1 rtview

Real-time viewer displays statistics for each of the ports.

When first entering rtview a lit of the currently enabled IPT applications is displayed. Some of these applications, such as the protocol servers, support pressing right-arrow to view the program threads.

The up and down arrows are used to move between ports. The space bar can be pressed to get more detail about the port you are currently on. Press space again to get back to the port list. Certain port setting changes will require a thread restart before the change takes effect. An example of this is changing the baud rate of a serial port. In order to minimize downtime, the IPT allows individual threads to be restarted so that the other ports may continue processing packets, while you make changes. To stop a thread, use the cursor navigation keys to highlight the thread you want to change. The press <F6> to stop the thread. You should see the status change to PAUSE and then to STOPPED. Once the thread says STOPPED, you may press <F7> to restart it. It is now possible to clear the stats for the current port. Just press the DEL key to clear the counters. To clear the stats for ALL ports, press <SHIFT><DEL>. If for some reason the screen gets out of sync, pressing <CTRL><R> will redraw the screen.

Chapter 5

System Integration

5.1   Encoder Input Protocol

The encoder listens on a TCP packet for a specially formatted packet. Some of the fields in the packet are TNPP-like, but the packet is not compatible with TNPP packet.

The incoming packet may be up to the BUFFSIZE in the encoder section of ipt.ini. A value of 256k can be used to allow for enough space for a 30 second voice message.

Below is a description of the incoming packet:

Field	Format	Description
Packetsize	uint32	Packet size (length of data to follow)
Pagetype	printchar	P=P512,p=P1200,Q=P2400,G=Golay,T=GolayIIA, F=Flex,5=5tone,2=2tone
Pageclass	printchar	B=tone,N=numeric,A=alpha,V=voice
Channel	01ABCDEF	channel 0-63 (or with 0x40 to make printable)
Function	0100ABCD	function 0-15 (Golay auto-adds 1 to make 1-4)
Repeat/Priority	01AVPPPP	A=repeatpage,V=repeatvoice,priority 0-15
Capcode length	010ABCDE	length of capcode field (0-31)
Capcode	variable	(F12345 for 5-tone no preamble)
Message	variable	message text or binary audio data

The Packetsize is a 4-byte unsigned integer in network byte order (use htonl to convert host to network byte order). It is the length of the data to follow the 4-byte packetsize and does not include the 4-byte packet size header.

To send a voice message the Message field must contain the binary audio data in
the following format: 8-bit unsigned linear, 8000 samples per second, mono.

Send your messaging packets to the ipt on the LISTEN_PORT defined in the [en-
code] section of ipt.ini.

Chapter 6

Troubleshooting

The IPT can be configured to keep very detailed logs for troubleshooting customer or connectivity issues. These logs are stored in the /var/log/debug directory in a sub-directory using a format of YYYY-MM-DD named for the date the debug information was written. For example, April 14th, 2006's debug logs are stored in the directory /var/log/debug/2006-04-14. Inside this sub-directory there are files for each thread of each program running.

6.1 Operating system

6.1.1 Bootup Issues

First determine if it is a computer issue or boot issue. Does the computer power on? Does the system appear to startup, but cannot find the operating system?

6.1.2 Network issues

By default the IPT is setup to obtain an IP address and domain settings automatically from a DHCP server. In order to use the IPT to accept connections from the Internet, a static IP should be used. This static IP address may be assigned by a DHCP server or in the IPT configuration files. See the "Network settings" section in the "Installation" chapter for information on setting the IP address and verifying that it is setup correctly. For more information you may use the following commands:

```
netstat
ping
traceroute
```

6.2   Application

6.2.1   Interpreting the debug logs

The debug logs contain a wealth of information for troubleshooting customer or port
setup issues. All debug entries are prefixed with a timestamp. This timestamp has
millisecond accuracy for determining with sub-second accuracy how much time has
elapsed between each event in the log. When DEBUG_FUNCS is enabled each time a
function is called a debug entry is added showing the name of the function and some
possibly important parameters. These lines can be recognized because they start
with **in** after the timestamp. Other important lines are the ComRead, ComWrite,
NetRead, and NetWrite lines. These come in various forms like ComWriteString and
NetReadBlock. The Com functions handle RS-232 port routines and the Net func-
tions handle network connections. Other lines are also logged that show additional
information.

6.2.2   Message queues

The IPT uses POSIX Message Queues for internal communications in the TNPP
and SMPP servers. To view certain message queue information type the following:

```
mkdir /dev/mqueue
mount -t mqueue none /dev/mqueue
```

Additional information on the system message queues is in the `/proc/sys/fs/mqueue`
directory.

Chapter 7

Change summary

7.1   Version 2.32 2011.07.20

- remove subscriber/pager sort from startup to iptconfig writes

- voicemodem improvements

- increase max baud on ports from 115200 to 460800.

- iptconfig allow more that 5 pager/subaccess/subsrcibers

- support blank line delimiter for rawinput mode

- showlog add -p to prevent message output

- showlog add -c to CSV output

- iptconfig #8->#12 support to connect to Hark Tunnel Server

7.2   Version 2.31 2011.07.20

- added rawinput mode to allow taking raw text in and paging it out - requires port based routing

7.3   Version 2.30 2011.07.20

- rtview.display_desc shows port desciption instead of device

- mode license/feature keys from ini to /usr/local/license.d directory

- support for returning reason codes on modem NO CARRIER

7.4   Version 2.29 2011.07.20

- added support for SOM-3517 CPU

- TNPP linktest go out in SIMPLEX if Tidle != 0

7.5   Version 2.28 2011.07.20

- add port notification and backup to allow port based routing

- improve POCSAG page queing to reduce IDLE codewords

7.6   Version 2.27 2011.07.20

- add tnppdest and inertia to encoder destprofile

- add TNPP routing support

7.7   Version 2.26 2011.07.20

- add support for max_msglen in destprofile

7.8   Version 2.25 2011.05.14

- add Advanced Transmitter Controller support

- archive debug files to thumb drive

- SNTP support for autosetting clock

- SSL now supports connect timeout like non-ssl connections

7.9   Version 2.24 2011.04.13

- TAP 1.8 compliance update

- mdmAnswer/mdmHangup speed improvements

- change webadmin to use html instead of xml

7.10 Version 2.23 2011.03.08

- POCSAG improve pagecue optimization

7.11 Version 2.22 2011.03.07

- support connect timeout for DNS lookup timeout

7.12 Version 2.21 2011.03.06

- add FLEX support to encoder

7.13 Version 2.20 2011.02.25

- web admin updates

7.14 Version 2.19 2011.02.21

- support purge debug hour -1 to purge every hour

- iptconfig add missing modem config menu

7.15 Version 2.18 2011.01.12

- encoder now supports receiving via TNPP CAP

7.16 Version 2.17 2011.12.15

- support port debuglevel

7.17 Version 2.16 2011.11.50

- always drop DTR to trigger DID modem shakeoff

7.18   Version 2.15 2011.09.22

- comwrite improvement for USB serial ports

- support sending non-standard port for HTTP/WCTP output

7.19   Version 2.14 2011.08.03

- only pad ID on left with zeros of %0..i

7.20   Version 2.13 2011.07.20

- send http created

7.21   Version 2.12 2011.06.23

- support WCTP SubmitRequest (in addition to SubmitClientMessage)

7.22   Version 2.11 2011.06.01

- support up to 63 serial ports (IPT-3U)

- support sending username and password

- support multiple page encoders (mainly for IPT-3U)

7.23   Version 2.10 2011.05.19

- Encoder POCSAG add sync and idle when page ends on a frame boundary

- web admin fixes

- support new encoder firmware

7.24   Version 2.9 2011.04.29

- bugfix NetClientOpen connect timeout wasn't working correctly

- add TAP alarm support - send alarm via TAP if go into dial backup

- SMPP support responding to UNBIND and ENQUIRE_LINK requests

- pad incoming ID on left with zeros if shorter than idformat width

- readd support for destprofile idformat (was only using idblock idformat)

- TAP set max message len for DID modems

7.25   Version 2.8 2011.03.31

- SNPP output now supports sending LOGIn command

- SMPP additions

7.26   Version 2.7 2011.03.15

- send arping to clear cached arp for quicker auto failover

- fix rtview display issues for some terminal emulators

7.27   Version 2.6 2011.03.11

- dynamically allocate page encoder structures so memory only used for protocols that are enabled

- add connecttimeout support to destprofile for timing out quicker and going to backup connection

- support sending SMS messages using cellular modem

- auto failover improvements

7.28   Version 2.5 2011.01.26

- add eth1 support

- send email alarm if error server not reachable

7.29   Version 2.4 2011.01.05

- iptconfig TAP profile ask for manual mode and DID modem option also

- don't retry outgoing TAP if rejected due to bad pager ID

- web admin fixes for subscriber/pager settings

- CONFIG SHOW_SUBLIST added for web paging - show list of pagers in the system

7.30   Version 2.3 2010.11.17

- add wall unit set time support

- bugfix-iptconfig TAP/TNPP add profile profilenumber not set

- bugfix-iptconfig update subscriber array size on add

- misc iptconfig additions

7.31   Version 2.2 2010.10.20

- support sending startup message

- send alarm if sequential test page missed (requires built in decoder)

- check_access now supports LDAP lookup

- now supports being built for Windows OS

- send_tnpp now supports CAP packets

- beginning of config.xml for web admin (not yet enabled)

- support DID modems for combined DTMF numeric and TAP dialup on DID trunks

- add filesystem watcher to send messages that show up in watched file

- tapothread communication improvements

- support SYSTEM_IDENTIFIER

7.32   Version 2.1 2010.09.03

- fix memory leak in redundant systems

- misc heartbeat fixes for redundant systems

- support individual IP_ALLOW per protocol

- check_access now supports require login for HTTP/WCTP

- onixd created to start and monitor/restart iptd if needed

- decode_mime support missing CRLF on last line (crashbug)

7.33 Version 2.0 2010.07.13

- move subscriber and subaccess from sqlite3 to ipt.ini

- add TNPP channel/zone to destprofile

- enhanced built-in encoder support

- *** NEW LICENSE KEY FORMAT ***

- computer interface

- redo ethernet config for better standby support

7.34 Version 1.11-1 2010.06.22

- fix tapprofile parsing (affected outgoing TAP)

- merge idblock into ipt.ini for easier backup and maintenance

- voice modem support for numeric paging over POTS lines

7.35 Version 1.10-1 2010.06.02

- convert utf-8 accented characters in from, subject, body to non-accented versions

- support utf-8 in from and subject =?utf-8?Q?...?=

- convert iso-8859-1 accented characters in from, subject, body to non-accented versions

- support iso-8859-1 charset in body

- support iso-8859-1 in from and subject =?iso-8859-1?Q?...?=

- decode_mime don't use strtok to parse email has problem seeing blank lines

- can now limit the amount of from and subject to use for the outgoing message

- CONFIG add MAX_FROM_LENGTH and MAX_SUBJECT_LENGTH

- SNPP out use DATA command if message has embedded CR or LF

7.36 Version 1.9-1 2010.05.22

- Support new CPU engine board

7.37   Version 1.8-1 2010.05.12

- RS-232 ports may now be configured to disallow idblock lookups

- Email replyto is now configurable per subscriber

- Email from address is now configurable

- process_tnpp now sets max_msglen

7.38   Version 1.7-1 2010.05.04

- Now supports running hot-standby redundant with IP address takeover

- Don't allow TNPP inertia less than 2

- iptconfig View syslog menu now works

- iptconfig Add real-time viewer to menu

7.39   Version 1.6-1 2010.04.20

- CONFIG add BROADCAST_SEND to support sending packet to multiple outgoing GCP ports

- iptconfig /etc/init.d/network is now /etc/init.d/networking

- iptconfig idblock, modem, and profiles add X to exit without saving

7.40   Version 1.5-1 2010.03.25

- add backup destinations

- add WCTP/SSL output support

- merge WCTP back into HTTP server

7.41   Version 1.4-1 2010.01.21

- TAP output support network connection

- add GCP output support

7.42 Version 1.3-1 2010.01.04

- tapothread only do modem dial and hangup if port is modem

- fix web page character counter

- TAP output support reinserting failed message back into queue

7.43 Version 1.2-1 2009.12.22

- tapithread support subsequent connections

7.44 Version 1.1-1 2009.12.14

- add TAP modem outdial support

7.45 Version 1.0-1 2009.04.07

- Initial release (merged code from isi and ipg with some features from omegalx)

Chapter 8

Warranty Information

For a period not to exceed one year from the date of purchase, Hark Technologies, guarantees that the electronic equipment sold will be fit for the ordinary purposes for which they are supplied, and will conform to the property description and statements of fact contained within any applicable brochure and labels provided with the product. However, upon the cessation of the one year warranty, Hark makes no warranty, expressed or implied, that the equipment is merchantable and/or fit for any particular purposes.

The Seller warrants that the goods covered by this agreement shall be free from defects in material and workmanship for one year when use under normal conditions and for the purpose for which they are sold. However, the warranty period for expendable parts, such as bulbs and fuses shall be limited to thirty days.

This warranty does not extend to damage incurred by natural causes such as lightning, fire, floods, or other catastrophes, damages caused by environmental extremes such as power surges and/or transients or willful, malicious, reckless, negligent acts or misuse by the purchaser or third parties.

All warranty work must be performed at Hark Technologies. No credit will be given for unauthorized repair work attempted by the customer or other unauthorized repair facilities. In/warranty merchandise must be shipped freight prepaid to the nearest Hark Technologies facility.

A Return Materials Authorization (RMA) Number must be obtained from Hark Technologies customer service department prior to returning any equipment, in-warranty, or otherwise to Hark Technologies for repair. Equipment received without the proper RMA number will be returned to the shipper.

All goods and materials are carefully tested and inspected before leaving the point of manufacture; however, as it is impossible to always detect imperfections, the only guarantee that is given by us, or for which we are in any way liable, is to repair or replace such goods as prove defective, when used for the purposes for which manufactured. All replaced goods are to be returned to us transportation prepaid. Under

no circumstances are we responsible for any other damages, incidental, consequential, or otherwise, nor in any case shall we be responsible for any damages beyond the price of the goods. No damages or charges of any kind, for labor, expenses, or otherwise suffered or incurred by the customer in replacing or repairing defective goods or otherwise occasioned by the customer will be allowed.

Written notice must be promptly given to the Seller of any perceived failure of the equipment sold, in order to fulfill the warranty, and in no event shall notice be given more than ten days after the discovery of the product defect. The notice shall state in what parts and wherein the warranty has failed and reasonable time shall be given to the Seller to remedy the difficulty. Failure to provide adequate notice within the required time frame shall be conclusive evidence of due fulfillment of the warranty on the part of the Seller, and that the product is satisfactory to the Purchaser, and that the Seller shall be released from all liability under the warranty.

DISCLAIMER OF WARRANTIES

THE WARRANTY PRINTED ABOVE IS THE ONLY WARRANTY APPLICABLE TO THIS PURCHASE. ALL OTHER WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTY OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED.

IT IS UNDERSTOOD AND AGREED THAT UNDER NO CIRCUMSTANCES SHALL THE SELLER BE LIABLE FOR ANY SPECIAL, INDIRECT, OR CONSEQUENTIAL DAMAGES, WHETHER THE THEORY OF LIABILITY IS BASED IN CONTRACT, TORT, UNDER ANY WARRANTY, OR IN NEGLIGENCE. THE PRICE AS STATED FOR THE WARRANTY IS A CONSIDERATION FOR LIMITING SELLERS WARRANTY. FURTHER, NO ACTION, REGARDLESS OF FORM, ARISING OUT OF THE TRANSACTIONS UNDER THIS AGREEMENT MAY BE BROUGHT BY THE PURCHASER MORE THAN ONE YEAR AFTER THE CAUSE OF ACTION HAS ACCRUED.

BREACH OF AGREEMENT

In the event that the terms or conditions of this Agreement are breached, then Hark is entitled to have the customer pay all reasonable court costs, attorney fees and expenses that shall be made or incurred by Hark in enforcing this Agreement; and the parties agree that the terms and conditions of this Agreement shall be binding on, apply and inure to their respective heirs, executors, administrators, successors and assigns.

This invoice shall be construed and governed by the laws of the State of South Carolina AND VENUE IN ANY LITIGATION PURSUANT TO THIS INVOICE SHALL BE IN DORCHESTER COUNTY, SOUTH CAROLINA.

ALTERATIONS AND CHANGES

Any alterations for deviations from the above specifications that involve extra material, costs or additional or more costly labor will require extra charges. These extra charges will be billed over and above the proposal amount.

PROPOSAL GOOD FOR THIRTY (30) DAYS

The price given in the proposal for material and labor is an offer that shall bind Hark for 30 days. If the proposal is not accepted within 30 days, then Hark has the option of revoking its proposal.

AGREEMENT SUBJECT TO APPROVAL BY MANAGEMENT

This offer is subject to management's approval. If terms of payment are: cash on completion, or if this is a credit sale, this offer is also subject to approval by Hark's credit manager.

ACTS BEYOND HARK'S CONTROL

Hark is not responsible for delays in delivery or for delays in installation due to weather, fire, strikes, governmental regulations, or other causes unforeseen or beyond it's control.

SECURITY AGREEMENT

Hark may require as a condition to this Agreement that the customer execute a security agreement to safeguard its position as a creditor in extending payment terms to the customer. In the event that Hark requires collateral, the customer agrees to provide a promissory note and a security agreement (and UCC-1) in the manner acceptable to Hark.

BAD CHECKS & C.O.D.

A service charge of $25.00 will be applied to each returned check. Accounts 60 days old will be placed on C.O.D. and technical service shall be withheld. Legal action will be taken after the account is 90 days old.

RETURNS

No returned goods will be accepted without a Returned Merchandise Authorization Number.

HANDLING/RESTOCKING CHARGE

A restocking charge of 20% will be made on all goods returned unless due to error caused by Supplier.

EQUIPMENT PACKING

Packing instructions: Equipment to be returned to Hark Technologies for repair must be packed in the original packing supplied by the factory. If the original packing is not available, Hark Technologies will provide it to you for a nominal fee. Customer packing materials can be used, providing the precautions are taken to provide adequate static protection for the equipment.

> DO NOT PACK HARK EQUIPMENT IN STYROFOAM PEANUTS ONLY

Repairs necessitated due to improper packing will be billed at the standard factory repair rate.

Hark Technologies will repair or replace equipment and return to customer, freight prepaid, within the continental United States. Equipment found not to be defective will be returned at purchaser's expense and will include cost of handling, testing and returning of equipment.

Out-of-warranty repairs will be billed at the established factory flat rate per hour, plus components needed for replacement.

TITLE

Title to and all goods or material hereafter purchased shall remain with Supplier until full purchase price has been paid.

ENTIRE AGREEMENT

This Agreement constitutes the entire agreement between the parties hereto; and this Agreement shall not be modified, amended, altered, or changed except by a written agreement signed by the party sought to be charged. However, change orders may be made by an oral agreement as enumerated in the "Alterations and Changes" section above.

Chapter 9

Cancellation

Buyer may by written notice to Seller within five (5) days of the merchandise received date cancel any contract or agreement arising here under, for other than the default of the Seller and at its convenience, in which the Buyer shall pay the Seller twenty percent (20%) of the above total price for all products and accessories as a restocking charge.

Index