

Internet Paging Terminal
Version 1.2

Hark Technologies

December 29, 2009

Copyright

Copyright © 1992-2009 Onix Electronic Systems Inc. All rights reserved. No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, photocopying, recording, or otherwise, without the prior written consent of Onix Electronic Systems Inc. d/b/a Hark Technologies 717 Old Trolley Rd Ste 6 #163, Summerville, SC 29485

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 FOREGOING 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

1	Introduction	7
1.1	Conventions used in this manual	7
1.2	Functional Overview	7
1.3	Features and Benefits	8
1.4	Support Services	8
2	Installation	11
2.1	Hardware	11
2.1.1	I	11
2.1.2	I	12
2.2	Operating System	12
2.2.1	Linux	12
2.3	System servers	12
2.3.1	sqlite3	13
2.3.2	postfix	13
2.3.3	Pound	13
2.4	Application	15
2.5	Database design	16
2.5.1	subscriber	16
2.5.2	Fields	16
2.5.3	subaccess	18
2.5.4	Fields	18
3	Configuration	19
3.1	System	19
3.1.1	Network configuration	19
3.1.2	DNS server	20
3.2	ipt.ini	20
3.2.1	[common]	21
3.2.2	[gcpd]	24
3.2.3	[httpd]	25
3.2.4	[passwd]	26
3.2.5	[rtview]	27
3.2.6	[smppd]	27
3.2.7	[smtpd]	28
3.2.8	[snppd]	30

3.2.9	[tapd]	30
3.2.10	[tnppd]	30
3.2.11	[wctpd]	31
3.3	Example ipt.ini	32
4	Database Maintenance	37
4.1	Command line	37
5	Database	39
5.1	subaccess	39
5.1.1	Fields	39
5.2	subscriber	41
5.2.1	Fields	41
5.3	pager	44
5.3.1	Fields	44
5.4	taprofile	46
5.4.1	Fields	46
5.5	tappassword	48
5.5.1	Fields	48
6	Program Descriptions	49
6.1	Introduction	49
6.2	System programs	49
6.2.1	onixd	50
6.2.2	syspage	50
6.3	Protocol servers	50
6.3.1	gcpd	50
6.3.2	httpd	51
6.3.3	isid	51
6.3.4	smppd	51
6.3.5	smtpd	51
6.3.6	snppd	52
6.3.7	tapd	53
6.3.8	tnppd	53
6.3.9	wctpd	53
6.4	Maintenance programs	56
6.4.1	rtview	56
7	Billing logs	59
8	System Integration	63
8.1	Encoder Input Protocol	63
9	Troubleshooting	65
9.1	Operating system	65
9.1.1	Bootup Issues	65
9.1.2	Network issues	65

9.2	Application	66
9.2.1	Interpreting the debug logs	66
9.2.2	Alarms	66
9.2.3	Message queues	66
9.3	Syslog server	67
10	Change summary	69
10.1	Version 1.1-1 2009.12.14	69
10.2	Version 1.0-1 2009.04.07	69
11	Warranty Information	71
12	Cancellation	75

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 8:00 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 expandability 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 set to 115200 N-8-1 and is wired the same as a PC RS-232 port. So if you are connecting to a PC you will need a null-modem cable.

2.1.1 I

PT-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 entry level systems that do not need a lot of expandability. It uses the same processor and has most of the capabilities of the 3U system.

The IPT-1U supports four RS-232 ports. The ports are numbered starting at the lower-left then lower-right then upper-left then upper-right when looking at the rear of the unit. 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. Only the bottom two ports

have modem control signals. The top two ports have TX, RX, and Ground.

An optional built-in modem is supported for dial backup and other uses.

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

2.1.2 I

PT-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.

2.2 Operating System

The IPT uses the Linux Operating System.

2.2.1 Linux

FINISHME System updates:

2.3 System servers

The IPT uses the Pound HTTP load balancer and reverse proxy. This allows for additional features such as SSL for secure communications between the client and server. Pound is configured to forward requests to an internal port for the built-in HTTP and WCTP server to accept.

Postfix and spamassassin are used to preprocess the incoming email and reduce the amount of spam sent to pagers.

Sqlite3 is use for the database. All subscriber information is stored in the database.

The setup of each of these servers will be described below.

2.3.1 sqlite3

No configuration needed. If the database does not exist the IPT will automatically create a new empty database. If an application update requires a database schema change it will be automatically applied when the new application version is started for the first time.

2.3.2 postfix

2.3.3 Pound

The Pound load balancer is used as a reverse proxy to handle HTTP and WCTP requests. This also allows the use of SSL for secure HTTP and WCTP.

To support SSL a secure certificate is required. You may self-sign your certificate which enables encryption to be used, but does not verify the authenticity of who you are connecting to. For WCTP this is not an issue, however clients connecting to the web server may get a warning in their web browser about not being able to verify the authenticity of the site. In order to prevent these warnings a certificate can be purchased from a commercial certificate authority like Verisign, Thawte, or Comodo for an annual fee.

First we need to generate the server key. When asked enter a passphrase for the server key. This should be something easy for you to remember because you will need it later in this process.

```
cd /usr/local/etc
openssl genrsa -des3 -out server.key 4096
```

To create a self-signed certificate follow the steps below then perform the steps to generate a certificate and import a certificate below.

- `openssl genrsa -des3 -out ca.key 4096`

This will generate a key for being a certificate authority. Use a phrase that is easy to remember, but hard to guess. You will need it later.

- `openssl req -new -x509 -days 3650 -key ca.key -out ca.crt`

Typically days will be 365, but we don't want to have to create a new certificate every year so use 3650 for 10 years.

- Enter pass phrase for ca.key:
- Country Name (2 letter code) [US]:

- State or Province Name (full name) [South Carolina]:
- Locality Name (eg, city) [Summerville]:
- Organization Name (eg, company) []:Hark Technologies
- Organizational Unit Name (eg, section) []:Internet Messaging
- Common Name (eg, your name or your server's hostname) []:ipt.harktech.com CA
- Email Address []:support@harktech.com

Creating the certificate request. This is used for both self-signed and authority signed certificates.

- `openssl req -new -key server.key -out server.csr`
 - Enter pass phrase for server.key:
 - Country Name (2 letter code) [US]:
 - State or Province Name (full name) [South Carolina]:
 - Locality Name (eg, city) [Summerville]:
 - Organization Name (eg, company) []:Hark Technologies
 - Organizational Unit Name (eg, section) []:Internet Messaging
 - Common Name (eg, your name or your server's hostname) []:ipt.harktech.com
 - Email Address []:support@harktech.com
 - A challenge password []:
You can just press enter to skip this
 - An optional company name []:
You can just press enter to skip this

Import the certificate. If you are using a certificate authority you will need to wait for their reply and save the certificate data on the system as a file named `ca.crt`. For self-signed certificates the `ca.crt` file will have been created by the instructions above.

- `openssl x509 -req -days 3650 -in server.csr -CA ca.crt -CAkey ca.key -set_serial 01 -out server.crt`

If you are using a self-signed certificate you can use 3650 for the days (or whatever you used above). However, if you are using a certificate authority the days will typically be 365.

The following steps will save a non-secure version of the server key so the server can start automatically.

- `openssl rsa -in server.key -out server.pem`

Next create the pound.pem file using the following command:

- `cat server.pem server.crt > pound.pem`

The configuration file is located in `/usr/local/etc/pound.conf`.

Example configuration file:

```
ListenHTTP
  Address 1.2.3.4
  Port    80
End

ListenHTTPS
  Address 1.2.3.4
  Port    443
  Cert    '/usr/local/etc/pound.pem'
End

Service
  URL './wctp'
  BackEnd
    Address 127.0.0.1
    Port    20081
  End
End

Service
  BackEnd
    Address 127.0.0.1
    Port    20080
  End
End
```

2.4 Application

The IPT consists of a master server which has a thread that listens for each supported protocol. As connections are received threads are spawned to process that connection. Real-time stats are available to see the activity for each thread.

2.5 Database design

2.5.1 subscriber

The subscriber table defines the subscriber and pager settings.

2.5.2 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.
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 incoming messages to callers that know the subscriber's caller passcode.
answertype	Not currently used.
allowservice	Specify with which protocols the subscriber is allowed to receive messages.
datecreated	Date the subscriber record was created. This field is automatically set when the record is created.
datealtered	Date the subscriber record was modified. This field is currently not automatically set when a record is modified.

maxmessagelen

The maximum message length the subscriber is allowed to receive. The default value is 240. Allowable values are from 1 to 990.

2.5.3 subaccess

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

2.5.4 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.
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.

Chapter 3

Configuration

3.1 System

3.1.1 Network configuration

The network configuration can be performed through the `iptconfig` utility that is displayed when you first login.

You can also 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.

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

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.

3.2 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.

3.2.1 [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.
0	No debug
1	Logging (a lot of miscellaneous debug info)
2	Functions (log entering functions)
8	Queues
16	Semaphores
32	ComLib (log serial port calls and info)
64	NetLib (log network calls and info)
128	Read
256	Write
4096	Tap Library logging
8192	Tnpp Library logging
16384	Thread information
32768	Telephony switching
65536	Web page template parsing
131072	Log reads of zero bytes also (not recommended)
262144	Message data (may create extremely large files)
524288	Telephony dial tokens
1048576	bin2str
2097152	Modem capabilities
4194304	HTTP admin sessions (not recommended)
8388608	Database open/close
16777216	Parse line
33554432	Interprocess communication
67108864	Trim silence
HOST_NAME	Fully qualified host name. This is written to /etc/hostname when the network configuration is updated.
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.
TRAFFIC_INTERFACE	The name of the main traffic ethernet interface. Typically eth0.
LICENSE_KEY	The license key for this system.
FEATURE_KEY	Specifies the licensed features for this system.
SYSPAGE_PORT	The TCP port number of the syspage server. This value must match the LISTEN_PORT in the [settings] section of the syspage.ini file installed on the system. See the syspage docs for more information.
CLEAR_STATS	Controls whether the remote IP address and last number are cleared from the real-time stats viewer. If you want to see the last connection in the real-time stats viewer set this to N (or 0) and the last IP address (for network connections) and last pager ID will remain on the screen until the next call comes in.
EMAIL_SUBJECT	The subject to use for outgoing emails if there is no subject on the incoming message.
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.
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.

COUNTDOWN_NOTIFY	Specifies the email address to send countdown limit exceeded emails to.
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_MESSAGE_LENGTH	The maximum length of incoming messages. Any messages longer than this are truncated on input.
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.
ALLOW_DOMAINS	A comma-separated list of domains for which we accept messages.
BILLING_FIELDS	Specify fields to write to billing logs. See the “Billing logs” chapter for the format and definition of this field.
BILLING_FORMAT	Specify the format of the fields to write to billing logs. See the “Billing logs” chapter for the format and definition of this field.

3.2.2 [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.
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.
PROTOCOL_OPTION		Specifies protocol options.
	134217728	0x08000000 Require login
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.
VERSION		The GCP protocol version we report when asked via the @RV or @rv command.

3.2.3 [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. 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.
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.
SESSION_EXPIRE	The amount of time in minutes before the HTTP session times out.

3.2.4 [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 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.
DEFAULT_PROFILE	The default passthrough profile to use if one is not specified in the port definition.

3.2.5 [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.

3.2.6 [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	Maximum number of pages to keep in the processing queue at a time. Once this value is reached the queue will stop being processed until we drop below QUEUE_PERCENTAGE of this value.
QUEUE_PERCENTAGE	Percentage of queue to drop below before re-enabling output processing for a particular device.
RLIMIT_NOFILE	The maximum number of files the process is allowed to have open at a time. Typical Linux default is 1024. A good setting for a medium sized system is 8192. Large systems may need to use 32768.
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.
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.

3.2.7 [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.
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.
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.

3.2.8 [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.

3.2.9 [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.

`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.

3.2.10 [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	Maximum number of pages to keep in the processing queue at a time. Once this value is reached the queue will stop being processed until we drop below QUEUE_PERCENTAGE of this value.
FAULTOFF_INPUT	If this is enabled and the outgoing TNPP port faults off, the port the packet was received on will also be disabled. Normally this field is set to disabled.
RLIMIT_NOFILE	The maximum number of files the process is allowed to have open at a time. Typical Linux default is 1024. A good setting for a medium sized system is 8192. Large systems may need to use 32768.
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.

3.2.11 [wctpd]

Wireless Communications Transfer Protocol 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.
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.


```
[encode]
DEBUG_LEVEL=0x0000ffff
LISTEN_PORT=1259
BUFFER_SIZE=256k
PROTOCOL_OPTION=0
READ_TIMEOUT=30000:2000
MAX_QUEUE_ENTRIES=16
SERIAL_PORT=/dev/tts/5
SERIAL_BAUD=115200
TWO_TONE_GAP=0
TWO_TONE_TIMEOUT=5
FIVE_TONE_TIMEOUT=5
POCSAG_TIMEOUT=4
GOLAY_TIMEOUT=4
PING_INTERVAL=5
TONE_GAP=250
EC_STATIONID=Hark UPE
EC_KEY_STATES=0b00111000
EC_MTONE_HI=2200
EC_MTONE_LO=1200
EC_MBIT_SHIFT=0
EC_VBIT_SHIFT=1
EC_MHILO=0
EC_GUARD_TONE=0
EC_GTONE_DELTA=2175
EC_ITONE_DELTA=1800
EC_DATA_INVERT=1
EC_ID_INTERVAL=900
EC_KEY_UP_DELAY=250
EC_KEY_DIGITAL=100
EC_KEY_ANALOG=100
EC_KEY_DOWN_DELAY=50
EC_MAX_PACKET=1024
EC_PURC_ANALOG=2175,1950
EC_PURC_DIGITAL=2175,1950
EC_ANALOG_HLGT_TIME=120
EC_DIGITAL_HLGT_TIME=120
```

```
[gcpd]
DEBUG_LEVEL=0x0000ffff
LISTEN_PORT=3021
BUFFER_SIZE=1k
PROTOCOL_OPTION=0
READ_TIMEOUT=30000:2000
VERSION=6.100
```

```
[httpd]
DEBUG_LEVEL=0x0000ffff
LISTEN_PORT=20080
PROTOCOL_OPTION=0
BUFFER_SIZE=64k
READ_TIMEOUT=30000:1000
SESSION_EXPIRE=40320
```

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

```
[smppd]
DEBUG_LEVEL=0x0000ffff
LISTEN_PORT=2775
BUFFER_SIZE=16k
READ_TIMEOUT=30000:1000
```

```
[smtpd]
DEBUG_LEVEL=0x0000ffff
LISTEN_PORT=20025
BUFFER_SIZE=16k
PROTOCOL_OPTION=0
READ_TIMEOUT=30000:2000
MAX_RECIPIENTS=10
SPAM_HEADER=X-Spam-Score
SPAM_LEVEL=3
SPAM_ACTION=DISCARD
SPAM_BOOLHEADER=X-Spam-Flag
FORWARDED_FOR_HEADER=X-Forwarded-For
THROTTLE_CODE=451
```

```
[snppd]
DEBUG_LEVEL=0x0000ffff
LISTEN_PORT=444
PROTOCOL_OPTION=0
BUFFER_SIZE=1k
READ_TIMEOUT=30000:1000
MAX_RECIPIENTS=10
```

```
[tapd]
DEBUG_LEVEL=0x0000ffff
LISTEN_PORT=8273
PROTOCOL_OPTION=0
BUFFER_SIZE=1k
READ_TIMEOUT=30000:1000
```

```
DEFAULT_PROFILE=1
```

```
[tappassword]
```

```
#password|profile
```

```
000001|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|0x03|2000|1000|10000|4000|8000|3|3|3|25|25
```

```
[tnppprofile]
```

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

```
# option 0x01=transcrc, 0x02=simplex
```

```
1|default|0|200|10000|10000|10000|60000|6|24|6|0
```

```
[tnppd]
```

```
DEBUG_LEVEL=0x0000ffff
```

```
LISTEN_PORT=8677
```

```
MAX_QUEUE_ENTRIES=64
```

```
QUEUE_PERCENTAGE=95
```

```
BUFFER_SIZE=4k
```

```
READ_TIMEOUT=30000:1000
```

```
[tnppprofile]
```

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

```
# option 0x01=transcrc, 0x02=simplex
```

```
1|default|0|200|10000|10000|10000|60000|6|24|6|0
```

```
[wctpd]
```

```
DEBUG_LEVEL=0x0000ffff
```

```
LISTEN_PORT=20081
```

```
PROTOCOL_OPTION=0
```

```
BUFFER_SIZE=64k
```

```
READ_TIMEOUT=30000:1000
```


Chapter 4

Database Maintenance

Currently the IPT requires modifying the SQL database directly.

4.1 Command line

The IPT database can be maintained using a standard SQL interface. To login to the database type `sqlite3 /opt/ipt/ipt.db`.

Chapter 5

Database

In addition to the ini file which controls global and program specific configuration, the OMEGA-LX uses a Postgresql database for system configuration and storage.

5.1 subaccess

Subscriber messaging access database. This will allow restricting WCTP access to only those users with a record setup in this table. SNPP also uses this table for verifying access using the LOGIn command.

5.1.1 Fields

username	An up to 32 character username.
password	An up to 32 character password.
accesslevel	The security level for this subscriber.
	0 No Access
	1 Send page
	5 View real-time stats
	10 Lookup subscribers
	20 Add subscribers
	30 Update subscribers
	40 Delete subscribers
	50 Reseller access
	60 Administrator
	255 Unlimited

badloginattempts	Stores the current number of bad login attempts for this user. If this value reaches the maxloginattempts access for this user will be disabled until an administrator resets the badloginattempts to 0. If there are badloginattempts, but the maximum has not been reached this counter will be reset to 0 on successful login.
maxloginattempts	Maximum number of bad login attempts the user is allowed before access is disabled.
accountnumber	Restrict user to only viewing mailboxes with this account number. Used for reseller web administration access.
sourceaddress	SMPP source address. Specifies a specific SMPP source address to use when a client sends a message using this subaccess login. Only support for incoming SNPP and WCTP.
domainname	Append domain name to recipient ID if specified. Used for supporting multiple brands when the subscriber doesn't specify an @domain portion to the recipient address.

5.2 subscriber

The subscriber table allows you to setup specific overrides for the idblock table.

5.2.1 Fields

subscriberid	The subscriber ID. This is typically the subscriber's 10-digit pager number without dashes or other punctuation.
enabled	Set to TRUE to allow this subscriber to receive messages are FALSE to prevent this subscriber from receiving messages.
password	An up to 16 character password for the subscriber access.
accesslevel	The access level for the subscriber.
accountnumber	Specify account number for this subscriber. Used in conjunction with accountnumber in subaccess to restrict reseller admin access.
name	The subscriber's name.
companyname	The subscriber's company name.
companyphone	The subscriber's company phone number.
techname	The subscriber's tech contact name.
techemail	The subscriber's tech contact email address.
techphone	The subscriber's tech contact phone number.
techfax	The subscriber's tech contact fax number.
callerpassword	Used to restrict who is allowed to send this subscriber messages. Not all paging protocols support caller password. Currently caller password is supported in SNPP and WCTP.

timezoneoffset	The number of hours and minutes from UTC. US Eastern time is -500. In this example, the -5 is the number of hours from UTC and the 00 is the number of minutes to support timezones that are not on hour boundaries.
daylightsaving	Specifies whether location uses daylight saving time during the summer. Arizona, for example, does not use daylight saving time.
allowsource	Specifies the sources that are allowed to send messages to this subscriber. For example, some subscribers may only wish to receive messages via WCTP and not email. The value for this field is computed by adding the values in the following list together: <ul style="list-style-type: none"> 1 GCP 2 HTTP 4 SMPP 8 SMTP 16 SNPP 32 TAP 64 TNPP 128 WCTP
twoway	Flag to indicate a two-way paging subscriber.
datecreated	Timestamp of when the subscriber was created.
datealtered	Timestamp of when the subscriber was last modified.
badloginattempts	Stores the current number of bad login attempts for this subscriber. If this value reaches the maxloginattempts access for this subscriber will be disabled until an administrator resets the badloginattempts to 0. If there are badloginattempts, but the maximum has not been reached this counter will be reset to 0 on successful login.

maxloginattempts	Maximum number of bad login attempts the subscriber is allowed before access is disabled.
callcount	Number of calls received by this subscriber.
countdownlimit	Maximum allowed calls per period.
countdowncurrent	The current countdown callcount.
countdowntype	The countdown type. 0=no countdown, 8=daily limit auto-reset at end of day, 10=monthly limit auto-reset at midnight of first day of month. A notification email can be sent to a customer support center email address so they know why a customer is calling to report a problem. In order to setup the email notification make sure that the COUNTDOWN_NOTIFY and SMARTHOST_NAME, SMARTHOST_PORT, and SMARTHOST_TIMEOUT are specified in the [common] section of omega.ini.

5.3 pager

The pager table contains optional paging records for the subscribers contained in the subscriber table. If a pager record does not exist for a subscriber the subscriber id is used for outgoing paging. However records may be added in this table for a subscriber to specify multiple delivery devices. For example, a TNPP pager and email. Multiple pager records are supported for each subscriber.

5.3.1 Fields

subscriberid	The subscriber id in the subscriber table this pager record belongs to.
sequencenum	A unique sequence number to use for this pager. The first pager should be sequence 1, next pager for this subscriber would be 2, etc.
enabled	Specify whether or not this pager record is currently enabled for message delivery.
outputgroup	The output group to use for delivery.
idcap	An up to 128 character id or capcode to deliver the message to. This field would also contain the full email address of the recipient for email delivery.
pagertype	TNPP CAP pager type (see TNPP 3.8 section 5.5.1).
pagerclass	TNPP CAP pager class (see TNPP 3.8 section 5.5.2).
pagerfunction	TNPP CAP pager function (see TNPP 3.8 section 5.5.5).
pagerpriority	TNPP CAP pager priority (see TNPP 3.8 section 5.5.5 or 5.10.6 for extcap).
rfchan	TNPP CAP RF channel (see TNPP 3.8 section 5.5.3).

rfzone TNPP CAP RF zone (see TNPP 3.8 section 5.5.4).

sendfields Specify which email headers to send out. Allowable values are F, S, B, C, and T. These may be combined. For example to send subject and body use SB.

- F From (email address)
- S Subject
- B Message Body
- C Word Count
- T Timestamp
- F From (“real name”)
- D Disposition-Notification-To

5.4 taprofile

A table of profiles for TAP. This allows the use of different timeouts and manual page prompts for different services. This table also supports specifying different timeouts when use in conjunction with the tappassword table.

5.4.1 Fields

profilenum	The profile number.
profilename	A descriptive name for this profile.
t1	Repeat CR until ID= (client). Default is 2000.
t2	Time after CR to wait for ID= (client). Default is 1000.
t3	Time to wait for packet response (client). Default is 10000.
t4	Time to wait for incoming packet (server). Default is 4000.
t5	Time to wait for ID= (server). Default is 8000.
n1	Number of CR to send looking for ID= (client). Default is 3.
n2	Number of packet resends (client). Default is 3.
n3	Number of ID= to send (server). Default is 3.
pageridprompt	Manual mode pager id prompt. Default is 'Pager ID? '.
messageprompt	Manual mode message prompt. Default is 'Message? '.
acceptedprompt	Manual mode accepted string. Default is 'Message sent.'.

rejectedprompt

Manual mode rejected string. Default is 'Send failed.'

5.5 tappassword

Allows custom TAP timeouts based on automatic mode password used.

5.5.1 Fields

password	The incoming automatic mode password. Typically this is a maximum of 6 characters, but the Omega supports up to 16.
name	A descriptive name for this password.
profile	The tapprofile to use for this password.

Chapter 6

Program Descriptions

The following sections describe the executables that make up the IPT application. For Linux systems the base directory is `/opt/ipt`.

6.1 Introduction

The Omega programs can be separated into different groups.

- Programs that must always be running. This is `onixd`.
- Programs that must be started depending on which services are to be enabled. For example, enable `tapd` for TAP protocol and `tnppd` for TNPP protocol. To enable incoming Internet email messages, `smtpd` must be started. To enable incoming Internet Simple Network Paging Protocol (SNPP) messages, `snppd` must be started.
- Maintenance programs that don't need to be running all the time. These are `rtview`, `sptest`, and `oservice`.

6.2 System programs

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

6.2.1 onixd

onixd is the master program that starts all of the other processes and then monitors the processes. If a process exits for some reason, onixd will restart it automatically.

6.2.2 syspage

syspage is the Omega alarm server. It accepts alarms on a TCP port and pages it out based on the rules in its configuration file. Please see the syspage manual for more information.

6.3 Protocol servers

6.3.1 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
- @CR create record
- @RE read record
- @DR delete record
- @MR modify record

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.

Other commands will return ?02 Unknown command. The lower-case versions of these commands are also supported. For example, the @CR command takes a two-digit field number for the key (e.g. @CR#01/) and the @cr command takes a three-digit field number for the key (e.g. @cr#001/).

This limited programming ability was added for billing systems which only support the Glenayre Computer Protocol.

6.3.2 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. Each virtual host supports a customizable directory.

6.3.3 isid

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 received to a capture file for the current day in the capture directory. The capture directory is accessible through the web admin page.

6.3.4 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.

6.3.5 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.

Message Disposition Notification

As of version 4.0-12 message disposition notification is supported. If a message is received with the RFC2298 Disposition-Notification-To header and the outgoing delivery type is email, the Disposition-Notification-To header will be added to the outgoing email with the value received from the sender.

As of version 4.0-15 this has been further enhanced to support the non-standard Microsoft Return-Receipt-To header. In addition 4.0-15 supports the ability to specify which of the two headers to send in the outgoing email.

If the incoming email contains both a Disposition-Notification-To and a Return-Receipt-To header the Disposition-Notification-To value will be used in the outgoing email using the header defined in the outgoing SMTP service record.

6.3.6 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 Omega will accept up to 16384 bytes per line, but some SNPP servers may be limited to as little as 1024.

The Omega 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>

6.3.7 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)

6.3.8 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.

6.3.9 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

6.4 Maintenance programs

6.4.1 rtview

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

When first entering rtview a list of the currently enabled Omega 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 Omega 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>. If for some reason the screen gets out of sync, pressing <CTRL><R> will redraw the screen.

Chapter 7

Billing logs

Each call processing application creates and maintains its own billing log file. Voice calls are logged in `vmail.in.txt`, tap is in `tapd.in.txt`, tnpp is in `tnppd.in.txt`, http is in `httpd.in.txt`, snpp is in `snppd.in.txt`, and smtp is in `smtpd.in.txt`. Outgoing pages are logged in files named after the protocol used. For example, email out will be in `smtp.out.txt`, snpp will be in `snpp.out.txt`, etc. These files can be found in the `logs` sub-directory of the Omega installation directory.

There are two variables to control the billing format and field configuration. These are `BILLING_FIELDS` and `BILLING_FORMAT`. Each program has its own settings for these fields in their respective section of `omega.ini`.

`BILLING_FIELDS` controls which logentry fields are written to the log file. This field can be up to 80 characters long. Not all tokens are supported by all protocols. The following are valid `BILLING_FIELDS` tokens:

S	subscriberid
f	senderid
F	remoteip
W	forwardedip
r	status
y	year (uses 2 digit year if field width < 4)
m	month
d	day
h	hour
i	minute
s	second

T	service
t	messagetext (up to 128 characters)
b	baudrate
l	messagelength
P	physicalport
L	logicalport
o	tnppsource
e	tnppdest
C	capcode (or ID if TNPP ID packet)
E	pagertype (encoding)
a	pagerclass (A=alpha, N=numeric, etc)
R	rfchan
Z	rfzone
+	callerid (ANI)
~	calledid (DNIS or DID)
#	messageid

BILLING_FORMAT specifies the locations and widths of each billing field. This field can be up to 512 characters long. Any non 'X' character is included in the billing record. The first character of each field is designated by an uppercase X and trailing characters by lowercase x's. The x's specify the width of each field in the billing record. Use a single uppercase X to output the field without padding or truncating. This is most useful for delimited files, otherwise extra characters (if wider than the specified billing width) are truncated.

Examples:

```
[smtpd]
BILLING_FIELDS=SFrhislLt
BILLING_FORMAT=Xxxxxxxxxx Xxxxxxxxxxxxxxxxxx Xxx Xx:Xx:Xx Xxxxx Xxx \
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
```

Would log the following to smtpd_in.txt on an incoming email from localhost:
5551212 127.0.0.1 ACC 08:20:13 00004 1 Test

```
[smtpd]
BILLING_FIELDS=SFrhislLt
BILLING_FORMAT=Xxxxxxxxxx,XXXXXXXXXXXXXXXXXX,Xxx,Xx:Xx:Xx,Xxxxx,Xxx,\
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
```

Would log the following to smtpd_in.txt on an incoming email from localhost:
5551212,127.0.0.1 ,ACC,08:20:13,00004,1 ,Test

```
[smtpd]
BILLING_FIELDS=SFrhislLt
BILLING_FORMAT=X,X,X,Xx:Xx:Xx,X,X,X
```

Would log the following to smtpd_in.txt on an incoming email from localhost:
5551212,127.0.0.1,ACC,08:20:13,4,1,Test

```
[smtpd]
BILLING_FIELDS=SFrhislLt
BILLING_FORMAT='X','X','X','Xx:Xx:Xx','X','X','X'
```

Would log the following to smtpd_in.txt on an incoming email from localhost:
'5551212','127.0.0.1','ACC','08:20:13','4','1','Test'

Status codes:

ACC = accepted
REJ = rejected

tapd:
E = database error
I = mailbox invalid
S = successfully accepted
T = timeout
C = bad checksum
B = bad block
F = TAP send failure
A = TAP send accepted

tnppd:
T = timeout
A = TNPP out - packet ACKed
n = TNPP receive - packet NAKed
2 = TNPP receive - duplicate packet (only if LOG_DUPS enabled)
f = TNPP receive - packet filtered CAN sent
a = TNPP receive - packet ACKed
d = TNPP receive - mailbox ID does not exist
i = TNPP receive - mailbox invalid
e = database error
c = TNPP receive - no output route for this destination
r = TNPP receive - all output queues full

R = TNPP send - received RS
N = TNPP send - received NAK
C = TNPP send - received CAN
F = faulted input

Chapter 8

System Integration

8.1 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 BUFSIZE 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 [encoder] section of ipt.ini.

Chapter 9

Troubleshooting

The Omega systems 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.

9.1 Operating system

9.1.1 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?

9.1.2 Network issues

By default the Omega is setup to obtain an IP address and domain settings automatically from a DHCP server. In order to use the Omega 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 Omega 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:

```
man netstat
man ping
man traceroute
man tcpdump
```

9.2 Application

9.2.1 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` functions handle network connections. Other lines are also logged that show additional information.

9.2.2 Alarms

Application alarms are sent to the syspage server running on the Omega. Syspage accepts alarms from the TNPP programs and sends alerts based on the settings in the `[syspage]` and `[alarm]` sections of the ini file. Syspage will log a copy of the alarm in the `/var/log/errors` directory in a file named after the program that generated the alarm. For example, `httpd.err` or `tnppd.err`. Syspage now supports also sending a copy of this alarm message to a serial port so you can send a copy to a separate alarm device if you wish. Alarm pages will also be sent based on settings in the `[alarm]` section of the ini file. These alarms can be paged out with the SMTP, SNMP, SNPP, or WCTP protocols.

Alarms are sent at various alarm levels. The following is a list of alarm levels:

32	Informational
64	Notice
128	Error
196	TNPP port fault-off and recover messages
240	Critical

Most systems are setup to email a copy of the alarms at error level 64 and above and set to page out alarms at error level 128 and above. It is recommended that error level 196 and above are paged out as these are alarms that indicate a degraded service level.

9.2.3 Message queues

The OMEGA-LX 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.

9.3 Syslog server

Unix and Linux systems include a centralized system logger called syslog. The Omega includes a system logging and paging program called syspage, so we don't log much to syslog. The syslog logs are stored in `/var/log` and may be in sub-directories under `/var/log`. Syslog messages can also be forwarded to another system acting as a centralized logging server. Our ISI and IPG boxes, make much more use of syslog as they do not have an alarm pager such as syspage in them.

Chapter 10

Change summary

10.1 Version 1.1-1 2009.12.14

- add TAP modem outdial support

10.2 Version 1.0-1 2009.04.07

- Initial release

Chapter 11

Warranty Information

WARRANTIES

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 12

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

- ALLOW_DOMAINS, 24
- BILLING_FIELDS, 24, 59
- BILLING_FORMAT, 24, 60
- BUFFER_SIZE, 24–31
- CLEAR_STATS, 22
- COUNTDOWN_NOTIFY, 24, 43
- DEBUG_LEVEL, 21, 25–31
- DEFAULT_PROFILE, 27
- DEFAULT_THROTTLE, 24
- EMAIL_FORMAT, 23
- EMAIL_PREFIX_BODY, 23
- EMAIL_PREFIX_FROM, 23
- EMAIL_PREFIX_SUBJECT, 23
- EMAIL_PREFIX_TO, 23
- EMAIL_SUBJECT, 22
- FAULTOFF_INPUT, 31
- FEATURE_KEY, 22
- FORWARDED_FOR_HEADER, 29
- GCP, 24
- gcpd, 50
- HELO_NAME, 22
- HOST_NAME, 21
- HTTP, 25
- httpd, 51
- ipt.ini, 20
- isid, 51
- LICENSE_KEY, 22
- Linux, 67
- LISTEN_PORT, 25, 26, 28, 30, 31
- MASQUERADE_AS, 21
- MAX_MESSAGE_LENGTH, 24
- MAX_QUEUE_ENTRIES, 28, 31
- Message Disposition Notification, 51
- onixd, 50
- pager, 44
- PASSD, 26
- PROTOCOL_OPTION, 25, 32
- QUEUE_PERCENTAGE, 28
- READ_TIMEOUT, 25–27, 32
- RETRY_INTERVAL, 23
- RETRY_MAX_RETRIES, 23
- RLIMIT_MSGQUEUE, 22
- RLIMIT_NOFILE, 28, 31
- rtview, 27, 56
- SCAN_TIME, 27
- SESSION_EXPIRE, 26
- SMPP, 27
- smppd, 51
- SMTP, 28
- smtpd, 51
- SNPP, 30
- snppd, 52
- SPAM_ACTION, 29
- SPAM_BOOLHEADER, 29
- SPAM_HEADER, 29
- SPAM_SCORE, 29
- subaccess, 39
- subscriber, 41
- Support, 8
- syslog, 67
- syspage, 50
- SYSPAGE_PORT, 22
- TAP, 30
- tapd, 53
- tappassword, 46, 48
- taprofile, 46, 48
- THREAD_STACK_SIZE, 23, 28

TNPP, 30

tnppd, 53

TRAFFIC_INTERFACE, 22

Unix, 67

VERBOSE_LEVEL, 27

VERSION, 25

virthost, 51

WCTP, 31

wctpd, 53