OMEGA-LX Internet Messaging Gateway
Version 7.2-1

Hark Technologies

March 26, 2014

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

Omega consists of a combination of hardware and software uniquely designed to work in conjunction with a paging system to emulate the functions provided by an Internet paging gateway, TAP concentrator, and TNPP router.

In addition, the several beneficial applications are provided, but are not limited to the following:

- Provides a password protected World Wide Web interface for subscribers to maintain certain configuration settings such as their passcode, and enabling/disabling their pager.

- Provides an administrative web interface for the service provider to setup system configuration and subscriber information.

- Computer interface supports use of a separate billing system to setup subscribers automatically.

- Delivery of numeric, alpha, or e-mail messages to an Internet e-mail address, and vice-versa.

Advanced features allow you to define when a particular pager will be paged, depending upon the day of the week, the time, message type, and urgency of the message. For example, you may only want a particular pager to be paged on Saturday and Sunday and all other messages routed to a second pager.

The above features are programmed using the pager table that is discussed in detail later within this manual.

1.3   Features and Benefits

- Supports Numeric and Alphanumeric messages.

- Provides ability to specify a future delivery time for a message.

- Private security codes for each mailbox.

- Multiple paging devices per mailbox.

- Supports paging via GCP (Glenayre Computer Protocol), 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 paging via dialup modem, dedicated RS232, and TCP/IP (Internet) connections. Backup all alphanumeric and numeric messages to one or more Internet e-mail addresses per mailbox.

- Send an e-mail to a pager.

- Accepts incoming alpha pages via GCP, TAP, TNPP, HTTP, SMPP, SMTP, SNPP, and WCTP.

- Delivery of numeric, alphanumeric, and e-mail messages to an Internet e-mail account, or accept these message types from the Internet.

- Web interface for sending text messages to pagers

- Web interface allows message viewing and maintenance of subscriber information.

- SSL support for HTTP and WCTP

1.4 Support Services

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

The support email address listed below 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:	678-242-5266
Fax:	678-242-5201
Web:	`http://harktech.com`
Sales email:	sales@prism-ipx.com
Support email:	prism-harktech_support@prism-ipx@harktech.com

Chapter 2

Installation

This chapter describes the initial installation of the operating system and system servers for software only Omega-LX systems. The site specific configuration that is used ofter this installation and also for configuring turnkey systems is in the next chapter named "Configuration".

> Note: If you are installing a telephony system please read the "Telephony" chapter before continuing. It has important information about specific versions of drivers and operating system installation.

2.1 System Requirements

The following equipment represents the minimum configuration for a base 32 port system.

- Pentium Dual-core or higher computer with 2 Gig RAM

- 160 Gig SATA hard drive

- One Ethernet card (used to connect to the Internet). Clustered systems require two (one preferably gigabit Ethernet).

- DVD-RW drive or tape drive for backups.

- Edgeport USB serial hub. USB serial ports are used so that additional ports can be added without having to shutdown the system and add additional boards in the computer.

- Comtrol DeviceMaster ethernet serial server. Provide serial ports in a clustered system.

- Fulltime (dedicated) internet connection with static IP address and internet domain name setup with MX record for email services. Dialup connections to internet are not supported. *

> Note: When using SATA hard drives make sure to get the Enterprise version. Desktop hard drives may not always give optimal performance in a 24x7 operation. We have been using Seagate Constellation drives lately with excellent results.

* It is difficult to judge how much bandwidth you will need initially. We suggest that you allow yourself the option to upgrade your Internet connection without penalty from your Internet Service Provider (ISP). For SMTP and SNPP, a 56k leased line is more than adequate for thousands of subscribers. Omega is designed to handle up to 1000 simultaneous SMTP connections and 1000 SNPP connections at the same time. These sessions are normally very short, so a large amount of traffic can be handled with the base system. However, adding the Web services can dramatically increase the amount of bandwidth required. If only Web-based paging is offered, the base 56k can handle the additional traffic without a problem. However, the 56k may not suffice if the Web-based database maintenance and message handling is used. There are several options available now, the most reliable being a dedicated leased line. However, SDSL will probably suit most businesses just fine. Internet connectivity can usually be purchased in increments of 64K. This is usually done with a fractional T1 connection. For example, you can start with 128K and upgrade to 256K or all the way to a full T1 at 1.544 Mbps.

Operating Systems supported:

- Centos Linux 6.x

2.1.1   Turnkey systems

Server

- Intel based server

  - Supermicro X9-SCA Motherboard
  - Intel Xeon E3-1230 Processor
  - 4GB ECC RAM
  - Redundant 500GB hard drives

- Centos Linux 6 x86_64

- Dimensions: 19in W x 7in H x 20in D

- Power: -48VDC @ 6A - Total system power requirement is a maximum of 6 amps. Redundant power supplies will need two 48V sources, each capable of 6 amps as the system may run from a single supply. Actual typical usage is 0.7 to 0.9 Amps per power supply module when both are running and 1.5 Amps when only one supply is enabled.

- These specifications are subject to change especially with regards to the motherboard, processor, memory, and hard drive configuration.

Features

See the "Protocol Servers" section in "Program Descriptions" chapter for detailed information.

- Glenayre Computer Protocol (GCP) version 6.0, 6.1, 8.0

- Hypertext Transfer Protocol (HTTP) version 1.0, 1.1

- Short Message Peer to Peer (SMPP) version 3.3, 3.4

- Simple Mail Transfer Protocol (SMTP)

- Simple Network Paging Protocol (SNPP) RFC 1861

- Telocator Alphanumeric Protocol (TAP) version 1.9

- Telocator Network Paging Protocol (TNPP) version 3.8.1

- Wireless Communications Transfer Protocol (WCTP) version 1.1

Capacities

- 200 simultaneous network connections per protocol

2.2 Hardware

The system may arrive in multiple boxes depending on the options ordered. After unpacking the server, inspect for any hidden physical damage. This should include opening the computer case and inspecting for any parts that may have worked loose during shipping. After inspecting all the equipment, start by mounting the server and any rack-mount accessories in your rack. The computer chassis was selected so that it can be mounting using only its front ears if you wish. You may also use slide rails if your application requires it. Connect the power cables, keyboard, video, and network cables. A mouse isn't required for operation, but one is included.

Clustered systems will include a second server and cables to connect the two computers together. After mounting the second server connect the included cross-over ethernet cable between eth1 on both computers. Eth1 is the ethernet connector to the right when looking at the back of the computer. Clustered systems also include a rack-mount KVM (Keyboard-Video-Mouse) switch box to switch the video and keyboard between the two clustered systems.

2.3 Operating System

The OMEGA-LX supports the Linux Operating System. Turnkey systems will already have the operating system and application software installed. However, software only systems will need to have the operating system installed and setup. Both configurations will need to have a few settings customized for your particular installation. Some configurations may not be available in all operating systems.

2.3.1 Installation

Centos Linux 6 can be downloaded from `http://www.centos.org`.

Make sure that you have a keyboard, mouse and monitor plugged into your server. Also make sure you have an Ethernet cable plugged in and you can reach the Internet. The following procedure will guide you through the Linux Operating System installation.

- Power on the computer and make sure that your BIOS settings are set to boot from CD before the hard drive.

- Insert the Linux System Installation DVD.

- Boot the computer. You will see a Centos 6 screen with the following:

  ```
  [F1 - Main][F2 - Options][F3 - General][F4 - Kernel][F5 - Rescue]
  boot:
  ```

- At the boot prompt press <ENTER> to install. At this point you will see a bunch of text scrolling on the screen.

- Next a text window asking if you would like to check the media appears. The media is tested before it is shipped, but if you want to make sure you can press <ENTER> to check the media. Or just press <RIGHTARROW> and press <ENTER> on Skip.

- Next you will see a few more lines of text, then the graphical installer will startup.

- Click Next

- You should see a language selection. Click Next to select the default of English. Otherwise select your language and click Next.

> Note: Hark can only support English installations

- Another language selection. This time the default is U.S. English. Click Next.

- Select "Basic Storage Devices". Click Next.

- If this is a new hard drive, you may see a popup window that says "The partition table on device sda was unreadable. To create new partitions it must be initialized, causing the lossof ALL DATA on this device." ... "Would you like to initialize this drive, erasing ALL DATA?". Click Yes.

- "Please name this computer" Hostname: omegalx-pri.harktech.com. Choose a hostname that fits in your domain.

- "Select time zone". Please select a city that is in your same timezone. It does not have to be the exact city you are in, unless your city has different timezone rules than the timezone you are in.

- "Root password". Enter a password for the root user. This is the password for the main system administrator.

- You should now see the disk partitioning screen. Select the "Create custom layout" radio button and click Next.

Single Hard Drive Installation

Perform the following steps for a single disk installation. See the RAID 1 section immediately after this section for mirrored drive installation.

- You should now be in Disk Druid. Click Create to create a new partition. Select "Standard partition". Click Create.

- You should now see the "Add partition" window.

- Set the mount point to /boot. Make sure the size is set to 500. Check the "Force to be a primary partition" checkbox. Click OK.

- Click Create to add another partition. Select "Standard partition". Click Create.

- Set the mount point to /. Set the size to 20000. Click OK.

- Click Create to add another partition. Select "Standard partition". Click Create.

- Set the filesystem type to swap. Set the size to 4096. Click OK.

- Click Create to add another partition. Select "Standard partition". Click Create.

- Set the mount point to /var. Set the size to 10000. Click OK.

- Click Create to add another partition. Select "Standard partition". Click Create.

- Set the mount point to /var/log. Set the size to 10000. Click OK.

- Click Create to add another partition. Select "Standard partition". Click Create.

- Set the mount point to /opt. Set the size to 20000. Click OK.

- Click Create to add another partition. Select "Standard partition". Click Create.

- Set the mount point to /var/opt. Check the "Fill to maximum allowable size" checkbox. Click OK.

- Click Next

- The "Writing storage configuration to disk" screen is displayed. Click "Write changes to disk".

- The "Install bootloader on /dev/sda" is displayed. You don't need to change anything here. Just click Next.

Mirrored Hard Drive Installation

Perform the following steps for RAID 1 (disk mirroring) installation.

- Click Create to add another partition. Select "Standard partition". Click Create.

- You should now see the "Add partition" window.

- Change File system type to "Software RAID". Set the size to 500. Uncheck the second hard drive (typically /dev/sdb). Check the "Force to be a primary partition" checkbox. Click OK.

- Change File system type to "Software RAID". Set the size to 500. Uncheck the first hard drive (typically /dev/sda). Check the "Force to be a primary partition" checkbox. Click OK.

- Click RAID to create the RAID device. Click OK for "Create RAID device". Change mount point to /boot. Change RAID Level to RAID 1. Click OK.

- Click Create to add another partition. Select "Standard partition". Click Create.

- Change File system type to "Software RAID". Set the size to 20000. Uncheck the second hard drive (typically /dev/sdb). Click OK.

- Change File system type to "Software RAID". Set the size to 20000. Uncheck the first hard drive (typically /dev/sda). Click OK.

- Click RAID to create the RAID device. Click OK for "Create RAID device". Change mount point to /. Change RAID Level to RAID 1. Click OK.

- Click Create to add another partition. Select "Standard partition". Click Create.

- Change File system type to "Software RAID". Set the size to 4096. Uncheck the second hard drive (typically /dev/sdb). Click OK.

- Change File system type to "Software RAID". Set the size to 4096. Uncheck the first hard drive (typically /dev/sda). Click OK.

- Click RAID to create the RAID device. Click OK for "Create RAID device". Change filesystem type to swap. Change RAID Level to RAID 1. Click OK.

- Click Create to add another partition. Select "Standard partition". Click Create.

- Change File system type to "Software RAID". Set the size to 10000. Uncheck the second hard drive (typically /dev/sdb). Click OK.

- Change File system type to "Software RAID". Set the size to 10000. Uncheck the first hard drive (typically /dev/sda). Click OK.

- Click RAID to create the RAID device. Click OK for "Create RAID device". Change mount point to /var. Change RAID Level to RAID 1. Click OK.

- Click Create to add another partition. Select "Standard partition". Click Create.

- Change File system type to "Software RAID". Set the size to 10000. Uncheck the second hard drive (typically /dev/sdb). Click OK.

- Change File system type to "Software RAID". Set the size to 10000. Uncheck the first hard drive (typically /dev/sda). Click OK.

- Click RAID to create the RAID device. Click OK for "Create RAID device". Change mount point to /var/log. Change RAID Level to RAID 1. Click OK.

- Click Create to add another partition. Select "Standard partition". Click Create.

- Change File system type to "Software RAID". Set the size to 20000. Uncheck the second hard drive (typically /dev/sdb). Click OK.

- Change File system type to "Software RAID". Set the size to 20000. Uncheck the first hard drive (typically /dev/sda). Click OK.

- Click RAID to create the RAID device. Click OK for "Create RAID device". Change mount point to /opt. Change RAID Level to RAID 1. Click OK.

- Click Create to add another partition. Select "Standard partition". Click Create.

- Change File system type to "Software RAID". Uncheck the second hard drive (typically /dev/sdb). Check the "Fill to maximum allowable size" checkbox. Click OK.

- Change File system type to "Software RAID". Uncheck the first hard drive (typically /dev/sda). Check the "Fill to maximum allowable size" checkbox. Click OK.

- Click RAID to create the RAID device. Click OK for "Create RAID device". Change mount point to /var/opt. Change RAID Level to RAID 1. Click OK.

- Click Next

- The "Writing storage configuration to disk" screen is displayed. Click "Write changes to disk".

- The "Install bootloader on /dev/sda" is displayed. You don't need to change anything here. Just click Next.

Install packages

- Make sure "Minimal" is checked.

- Click Customize Later

- Click Next to begin installation

- When packages are finished installing remove the DVD and click Reboot

After rebooting login as root. We now have a script that performs many of the manual steps in previous releases. Unfortunately, as installed the Minimal setting for CentOS doesn't bring up the network interface. Do the following steps to configure the network and get the initial configuration script:

Edit the `/etc/sysconfig/network-scripts/ifcfg-eth0` file and change NM_CONTROLLED=no, also change ONBOOT=yes. Also, add BOOTPROTO=dhcp and NOZEROCONF=yes. If you are installing a clustered system, set BOOTPROTO=none for a static IP address and add IPADDR and NETMASK lines with the proper static IP address and netmask.

Edit the /etc/sysconfig/network file and remove the domain name portion of the
HOSTNAME line. An alternative method is to do the following:

```
sed -i.bak 's/\.[a-z].*//g' /etc/sysconfig/network
```

Now restart the network interface and install additional packages:

```
service network restart
yum -y install wget
chkconfig auditd off
chkconfig netfs off
cd
wget http://support.harktech.com/dl/rhel6-x86_64/\
elrepo-release-6-5.el6.elrepo.noarch.rpm
wget http://support.harktech.com/dl/rhel6-x86_64/epel-release-6-8.noarch.rpm
wget http://support.harktech.com/dl/rhel6-x86_64/pgdg-centos92-9.2-6.noarch.rpm
rpm -ivh *.rpm
yum -y update
yum -y install ntp pciutils usbutils smartmontools openssl-clients \
libftdi drbd84-utils kmod-drbd84
ntpdate 0.centos.pool.ntp.org
chkconfig ntpd on
service ntpd start
hwclock --systohc --utc
```

The following is most likely not needed when installing minimal with CentOS 6.4
and higher:

```
yum -y erase matahari\* qpid\* sigar polkit dbus boost\* ConsoleKit\* \
eggdbus libicu
```

Most likely the above installed a new kernel so reboot now by entering `reboot`.

If this is a RAID 1 system, the system has been building the initial array since the
system was booted. To allow the system to complete rebuilding as quickly as possible
it is recommended to let the array finish building before rebooting the system. Type
`cat /proc/mdstat` to check the status of the array rebuild.

2.4   Clustering

The Omega-LX can be configured to support clustering in an active-passive configuration. This is an extra cost option must be specified at the time of order and can not be added later. Clustering is the ability for a standby server to automatically take over in the event of a failure on the primary system.

In order to do this a couple of things needs to be handled. First, because this is an unattended fail-over serial ports for protocols like TAP or TNPP can not be directly connected to the Omega. For this reason Digi Etherlite or Comtrol DeviceMaster RTS 1U rack-mount serial servers are used. These devices are connected using a 10/100baseT connection to an ethernet switch. The Omega then connects to the serial server and access the com ports as if they are on the server itself. Second, the hard drive storage needs to be synchronized so when the server switches over to the backup it has all the information available as of the moment of switchover. This is done using a network block device. Think of this as network RAID-1 (disk mirroring over a network). Due to the potentially large volume of data the network block device communicates over its own dedicated gigabit ethernet link (eth1). Finally, a heartbeat between the two machines is needed so the server can tell which one it is supposed to be running on. This heartbeat runs over the dedicated private ethernet running on eth1.

The clustering system uses two identical computers with dual gigabit ethernet network ports. Ethernet port 0 (eth0) is setup to connect to your network. This requires a static IP address. Ethernet port 1 (eth1) is used for the network disk mirroring and cluster heartbeat.

Turnkey clustered systems also include a rack-mount KVM switch to allow the use of a single keyboard and monitor.

If you intend to use TNPP over UDP to a Glenayre paging terminal with the active-standby clustering feature there are a few details to be aware of. Because Glenayre uses TNPP over UDP the source UDP port and the destination UDP port must match. This means, for example, that the service must use a bind port of 3050 to talk to a Glenayre listening on port 3050. This is not a problem and has always been supported in the Omega-LX. The issue comes when you want to connect to two separate Glenayre paging terminals using the same port (e.g. 3050). Due to the way networking works you can not bind two Omega TNPP services to the same port on the same interface. So two IP addresses need to be used and set to the bind ip address in the service table. These two IP addresses can go out the same ethernet interface, there is no restriction there.

The next issue with this is when the system changes over to the standby server. In

order to support this two virtual IP addresses will need to be created. Then when the system moves between servers the two (or more) virtual IP addresses with the bound TNPP UDP services will move also and the two (or more) connections to the Glenayre paging terminals will function.

Note: If at any time you install a kernel update, the Comtrol DeviceMaster or the Digi Etherlite driver must be rebuilt after rebooting so that your serial ports will be seen. After rebuilding and installed the serial driver appropriate to your installation restart the omegalx service with 'service omegalx stop' then 'service omegalx start'.

2.4.1   Comtrol Devicemaster Serial Server

The Comtrol DeviceMaster is a network attached RS-232 port server. This box allows the serial ports to be connected to a device which can be accessed from the currently active server. There isn't a package for the Comtrol drivers. They must be downloaded, compiled, and installed. This work will have already been done on turnkey systems.

Download, compile, and install the current Comtrol driver using the following commands:

Note: The kernel-devel and gcc packages need to be installed to compile the nslink driver `yum -y install kernel-devel gcc`.

```
cd
wget
ftp://ftp.comtrol.com/dev_mstr/rts/drivers/linux/devicemaster-linux-5.03.tar.gz
tar xzvf devicemaster-linux-5.03.tar.gz
cd nslink
make
make install
```

See the Comtrol DeviceMaster section in the Configuration chapter for information on setting the IP address in the config file.

2.4.2   Digi Etherlite Serial Server

The Digi Etherlite is a network attached RS-232 port server. This box allows the serial ports to be connected to a device which can be accessed from the currently

active server.

Download, build, and install the current Digi driver using the following commands:

> Note: The kernel-devel, gcc, ncurses-devel, openssl-devel, and
> rpm-build packages need to be installed to build the digi dgrp
> package `yum -y install kernel-devel gcc ncurses-devel`
> `openssl-devel rpm-build`.

```
cd
wget ftp://ftp1.digi.com/support/driver/40002086_S.src.rpm
rpmbuild --rebuild 40002086_S.src.rpm
rpm -ivh /usr/src/redhat/RPMS/x86_64/dgrp-1.9-31.x86_64.rpm
```

See the Digi Etherlite section in the Configuration chapter for initial configuration information.

2.4.3   Firewall

Linux 2.6 and higher use the iptables firewall. On Omega-LX systems we enable this by default. If you add any TNPP over IP connections or other services running over the network you will need to add rules to allow that traffic into the system.

A sample iptables script is installed in /etc/sysconfig/iptables.hark and is shown below:

```
*filter
:INPUT ACCEPT [0:0]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [0:0]
-A INPUT -i lo -j ACCEPT
-A INPUT -i eth1 -j ACCEPT
-A INPUT -p icmp --icmp-type any -j ACCEPT
-A INPUT -p 50 -j ACCEPT
-A INPUT -p 51 -j ACCEPT
-A INPUT -p udp --dport 5353 -d 224.0.0.251 -j ACCEPT
-A INPUT -p udp -m udp --dport 631 -j ACCEPT
-A INPUT -p tcp -m tcp --dport 631 -j ACCEPT
-A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
-A INPUT -m state --state NEW -m tcp -p tcp --dport 22 -j ACCEPT
-A INPUT -m state --state NEW -m tcp -p tcp --dport 25 -j ACCEPT
-A INPUT -m state --state NEW -m tcp -p tcp --dport 80 -j ACCEPT
```

```
-A INPUT -m state --state NEW -m tcp -p tcp --dport 443 -j ACCEPT
-A INPUT -m state --state NEW -m tcp -p tcp --dport 444 -j ACCEPT
-A INPUT -m limit --limit 3/min -j LOG --log-prefix "fw-in: "
-A INPUT -j REJECT --reject-with icmp-host-prohibited
-A FORWARD -i lo -j ACCEPT
-A FORWARD -p icmp --icmp-type any -j ACCEPT
-A FORWARD -m state --state ESTABLISHED,RELATED -j ACCEPT
-A FORWARD -m limit --limit 3/min -j LOG --log-prefix "fw-for: "
-A FORWARD -j REJECT --reject-with icmp-host-prohibited
COMMIT
```

We allow everything from eth1 because this is typically the crossover ethernet connection on clustered systems.

The -A FORWARD rules are not necessary unless you are using this server as a firewall. We do not recommend using the Omega-LX as a firewall, because it is our belief that a firewall should have as few services running on it as possible. This means that the firewall only acts as a firewall and all other services are on systems behind the firewall.

2.4.4 Host file

Example /etc/hosts:

```
127.0.0.1       localhost localhost.localdomain localhost4 localhost4.localdomain
::1             localhost localhost.localdomain localhost6 localhost6.localdomain
10.0.0.1        omegalx-pri omegalx-pri.harktech.com
10.0.0.2        omegalx-sec omegalx-sec.harktech.com
```

2.4.5 SSH keys

In this section we will configure SSH keys to make copying files between the primary and standby server easier.

Perform the following steps on the primary server:

```
ssh-keygen -t rsa -f ~/.ssh/id_rsa -N ""
scp -p ~/.ssh/id_rsa.pub root@10.0.0.2:/root/.ssh/id_rsa.pub.pri
```

On standby server:

```
ssh-keygen -t rsa -f ~/.ssh/id_rsa -N ""
scp -p ~/.ssh/id_rsa.pub root@10.0.0.1:/root/.ssh/id_rsa.pub.sec
cat ~/.ssh/id_rsa.pub.pri >> ~/.ssh/authorized_keys
chmod 600 ~/.ssh/authorized_keys
```

Back on primary server:

```
cat ~/.ssh/id_rsa.pub.sec >> ~/.ssh/authorized_keys
chmod 600 ~/.ssh/authorized_keys
```

At this point you should be able to ssh from the primary to the standby and the standby to the primary over the eth1 crossover cable without needing a password.

2.4.6   Cluster Manager

Starting with version 7.0 the Omega-LX uses its own cluster manager. The cluster is specifically written to support the Omega-LX and switchover from the primary to the standby computer as quickly as possible. The cluster manager can be installed now using the following:

```
yum install omegacl
```

This will automatically install a resource file for DRBD (described in the following section.

The cluster manager configuration is in `/etc/omegacl/heartbeat.ini`.

Here is a sample heartbeat.ini:

```
[heartbeat]
DEBUG_LEVEL=0x0000ffff
PING_INTERVAL=2
PING_ADDRESS=192.168.1.1
PING_TIMEOUT=1000
PING_TRIES=2
SHUTDOWN_WAITTIME=10
VIRTUAL_IP=192.168.1.230
VIRTUAL_NETMASK=255.255.255.0
VIRTUAL_DEVICE=eth0
VIRTUAL2_IP=
VIRTUAL2_NETMASK=
VIRTUAL2_DEVICE=
PRIMARY_IP=192.168.1.231
STANDBY_IP=192.168.1.232
```

2.4.7 Drbd configuration

Drbd is the network disk mirroring. It is responsible for making sure that all of the disk writes are copied to the standby server so it will be up-to-date in case of fail-over.

Make sure eth1 is configured and up on both servers. Also, make sure that the host names used in the drbd config exist in the /etc/hosts file.

First, the drbd packages need to be installed. Make a note of the file system /opt is mounted on. This can be done with `df` or `grep /opt /etc/fstab`. Use this filesystem below with the sed command and the dd command.

Perform the following steps on both servers to install the drbd packages and perform the initial configuration:

```
umount /opt
sed -i 's:^/dev/md5:#/dev/md5:' /etc/fstab
chgrp haclient /sbin/drbdsetup /sbin/drbdmeta
chmod o-x /sbin/drbdsetup /sbin/drbdmeta
chmod u+s /sbin/drbdsetup /sbin/drbdmeta
dd if=/dev/zero of=/dev/md5 bs=512 count=10000
```

The /dev/md5 above must be replaced with the device the /opt file system is mounted on. For single drive system this will be something like /dev/sda3. If you are unsure type `grep /opt /etc/fstab`.

The network block device configuration is in /etc/drbd.d/omegacl.res. A sample will be installed with the omegacl package described above.

The following is an example configuration file:

```
resource omega {
  protocol C;

  handlers {
    pri-on-incon-degr "echo o > /proc/sysrq-trigger ; halt -f";
    pri-lost-after-sb "echo o > /proc/sysrq-trigger ; halt -f";
    local-io-error "echo o > /proc/sysrq-trigger ; halt -f";
    outdate-peer "/usr/sbin/drbd-peer-outdater";
  }
```

```
startup {
  wfc-timeout  5;
  degr-wfc-timeout 120;    # 2 minutes.
}

disk {
  on-io-error   detach;
}

net {
  after-sb-0pri disconnect;
  after-sb-1pri disconnect;
  after-sb-2pri disconnect;
  rr-conflict disconnect;
}

syncer {
  rate 50M;  # use 10M for 100Mbit network
  al-extents 257;
}

on omegalx-pri {
  device     /dev/drbd0;
  disk       /dev/sda3;  # set to where /opt is (e.g. /dev/md5)
  address    10.0.0.1:7788;
  meta-disk  internal;
}

on omegalx-sec {
  device     /dev/drbd0;
  disk       /dev/sda3;  # set to where /opt is (e.g. /dev/md5)
  address    10.0.0.2:7788;
  meta-disk  internal;
}
}
```

The two **on** sections are the most likely to need customizing for an installation. They have the hostname, the device, disk, and address configuration. The address in the file above is the IP address on the dedicated gigabit ethernet link. See the DRBD Configuration section in the "Configuration" chapter for more information on the site-specific configuration.

Now that the drbd resource file has been created and you have entered your site-specific changes, copy it to the standby server. The following commands assume that you have the crossover ethernet cable connected between the two servers on eth1:

```
scp -p /etc/drbd.d/omegacl.res root@10.0.0.2:/etc/drbd.d
```

We can now finish the initial config. Perform the following steps on the both servers:

```
chkconfig drbd on
service drbd start
drbdadm create-md omega
```

Now continue with the drbd configuration on the primary server only:

```
drbdadm adjust omega
drbdadm -- --overwrite-data-of-peer primary omega
mkfs.ext4 /dev/drbd0
tune2fs -c0 -i0 /dev/drbd0
mount /dev/drbd0 /opt
```

And perform the following steps on the standby server:

```
drbdadm connect omega
```

At this point the DRBD should be syncing between the two servers. You can check the status by typing `cat /proc/drbd` on either server.

2.5   System servers

The OMEGA-LX no longer uses the Postfix as a front end. The Postfix server can still be used for outgoing email though. To do this Postfix has been moved from port 25 to port 2525.

The OMEGA-LX uses the Postgresql database server for its database. All subscriber information, messages, and logs are stored in the database for easier replication, reporting, and maintenance. The setup of each of these servers will be described below.

2.5.1   Firewall - iptables

The firewall configuration is stored in /etc/sysconfig/iptables. A default configuration will already be installed. An OMEGA-LX specific sample configuration can be retrieved from our support server with the following:

```
cd /etc/sysconfig
wget http://support.harktech.com/dl/omegalx/iptables.hark
```

You can use this file for an example to change your existing iptables or overwrite the exiting iptables with `cp -p iptables.hark iptables`. After changing the iptables file the firewall will need to be restarted with `service iptables restart`.

If any network servers are created in the Omega-LX (e.g. a TNPP over TCP/IP server listening for connections) a new rule will need to be added to the firewall configuration to allow that connection. To do this copy one of the existing lines such as the one for port 444 (SNPP). Then modify the port number for the port your new service is listening on (e.g. 10000).

After making any changed to the iptables configuration restart the firewall with `service iptables restart`.

2.5.2   Database - Postgresql

Redhat Enterprise Linux 6.x and Centos 6.x use Postgresql 8.4 by default. The OMEGA-LX server uses Postgresql 9.2. In order to install Postgresql 9.2 in Centos 6.x the following steps must be performed:

The PGDG Postgresql RPMs are installed with the following:

```
wget http://yum.pgrpms.org/9.2/redhat/rhel-6-x86_64/pgdg-centos92-9.2-6.noarch.rpm
rpm -ivh pgdg-centos92-9.2-6.noarch.rpm
yum install postgresql92-server
echo 'pathmunge /usr/pgsql-9.2/bin' > /etc/profile.d/pgsql.sh
source /etc/profile
```

Create the sysconfig file for postgresql with the following:

```
cat > /etc/sysconfig/pgsql/postgresql-9.2 << EOF
PGDATA=/opt/pgsql
PGLOG=/opt/pgsql/pgstartup.log
PGOPTS=-i
EOF
```

Also do the following to update the postgres user environment:

```
cat > /var/lib/pgsql/.bash_profile << EOF
[ -f /etc/profile ] && source /etc/profile
```

```
export PGDATA=/opt/pgsql
export PGLOG=/opt/pgsql/pgstartup.log
EOF
```

The above will change the postgresql database directory from /var/lib/pgsql to /opt/pgsql. For clustered systems this will move the database to a filesystem that is replicated over drbd.

Create the new database directory and set permissions:

```
mkdir /opt/pgsql
chown postgres:postgres /opt/pgsql
```

Recent versions of the default SELinux policy requires the following commands to be run for the new Postgresql data directory:

```
yum -y install policycoreutils-python
semanage fcontext -a -t postgresql_db_t "/opt/pgsql(/.*)?"
restorecon -R -v /opt/pgsql
```

These commands are only required if selinux is set to enforcing (the default Red-Hat/Centos configuration.

You can verify the SELinux changes with:

```
grep -i pgsql /etc/selinux/targeted/contexts/files/file_contexts.local
ls -lZ /opt
```

Type the following to initialize and create the database:

```
su - postgres -c "initdb -D /opt/pgsql"
```

Now that the database has been initialized, edit the configuration file and enable TCP connections from the localhost. Make sure the following line is not commented out in **/opt/pgsql/pg_hba.conf**:

```
host    all         all         127.0.0.1         255.255.255.255   trust
```

In order to support load-balanced systems you will need to add a line for your private network. For example:

```
host    all         all         10.100.1.0/24    trust
```

The Omega-LX makes many simultaneous connections to the Postgresql server. Because of this certain server limits need to be increased. Edit `/opt/pgsql/postgresql.conf` and change max_connections and shared_buffers to the following (some sites may need larger values):

```
max_connections = 4000
shared_buffers = 128MB
```

> Note: The above settings require an increase in the default kernel limits. Please see the Kernel limits section in the Configuration chapter for information on increasing these limits.

Smaller systems, for example a hospital installation, may use the following settings:

```
max_connections = 1000
shared_buffers = 64MB
```

If you are running a clustered system the postgresql server will automatically be started by the cluster manager (heartbeat) so make sure postgresql is not set to automatically start by typing `chkconfig postgresql-9.2 off`.

If you are not running a clustered database server type `chkconfig postgresql on` to enable the service to automatically start on bootup.

For both clustered and non-clustered systems we need to start the postgresql server with `service postgresql-9.2 start` to perform the following steps on the **primary server only**:

```
su - postgres
createdb omegalx
createdb omegalog
createdb thinclient
exit
```

2.5.3   Email - Postfix

To use Postfix for outgoing email edit the /etc/postfix/master.cf file and change the smtp at the beginning of line 11 to 2525.

2.5.4 Anti-spam - Spamassassin

Spamassassin is installed by default, but not enabled. To enable spamassassin type `chkconfig spamassassin on`. This will set the spamassassin service to start automatically on boot up.

The default configuration is in /etc/mail/spamassassin/local.cf.hark. This can be copied to the running configuration with `cp -p /etc/mail/spamassassin/local.cf.hark /etc/mail/spamassassin/local.cf`. Then restart the spamassassin service with `service spamassassin restart`. The configuration chapter will have additional information for customizing this file.

The following is an example configuration:

```
required_hits 5
report_safe 0
rewrite_header Subject [SPAM]
add_header all Level _SCORE_

score __RFC_IGNORANT_ENVFROM 0.0
score DNS_FROM_RFC_DSN 0.0
score DNS_FROM_RFC_POST 0.0
score DNS_FROM_RFC_ABUSE 0.0
score DNS_FROM_RFC_WHOIS 0.0
score DNS_FROM_RFC_BOGUSMX 0.0

# Spamhaus DNSBL is not longer free for commercial or high-volume use
score __RCVD_IN_ZEN 0.0

# Pay-for DNSBL services
score RCVD_IN_MAPS_RBL 0.0
score RCVD_IN_MAPS_DUL 0.0
score RCVD_IN_MAPS_RSS 0.0
score RCVD_IN_MAPS_NML 0.0
```

2.6 Application

The OMEGA-LX consists of several applications working together to accept messages and forward them to their proper destination.

After the initial setup, the following steps need to be performed to install the Omega software.

2.6.1   Downloading and Installing

The omegalx can now be installed over the Internet. This applies to both licensed and demo versions. You will need port 80 and 443 open to the Internet to install, register, and/or update the omegalx. To install the omegalx over the Internet login to your Linux server as root and type the following commands:

```
cd /etc/yum.repos.d
wget http://support.harktech.com/dl/rhel6-x86_64/hark.repo
yum install omegalx
```

Chapter 3

Telephony

While we have supported telephony for many years in the Omega Unified Messaging Server, the Omega-LX was designed to be purely an Internet Messaging Gateway. In recent years the Omega-LX has been expanded to be more of a paging terminal replacement including the support of USB-attached paging encoders. Version 5.1 of the Omega-LX takes this even a step further and now supports numeric paging over T1 interfaces.

To support T1 interfaces the Dialogic (formerly Natural Microsystems) CG-6x6x boards are used. This includes the CG-6060 and CG-6565.

The Natural Access drivers for the CG boards may be downloaded and install with the following (as root):

```
cd
wget -N http://www.dialogic.com/files/natural-access/9.0.8/66-0321.tar.Z
mkdir nms_install
tar xzvf ../66-0321.tar.Z
echo 'Red Hat Enterprise Linux release 6.5' >> /etc/redhat-release
./install
chkconfig nms_cx2000 off
exec su -
```

You will need to reboot for the NMS license manager to start. You can quickly reboot with `init 6`.

Normally an NMS install will require configuring some files in /opt/nms. The Omega-LX will automatically generate these files based on the configuration in the telboard and teltrunk database tables.

Special note regarding system updates. If you upgrade your CentOS system such that a new release is installed (centos-release-6-x package is updated), you will need to echo the "Red Hat Enterprise Linux" line in the above install section before rebooting. If you don't the NMS driver will not load. You may also need to re-run the ./install above if the kernel version changes. This will need to be done after you boot with the new kernel. It is recommended that you not update the centos-release or the kernel when running NMS boards.

Chapter 4

Configuration

4.1 System

4.1.1 IP addresses

IP address configuration in CentOS (and other RedHat-based Linux) is defined in several scripts in the /etc/sysconfig directory. First, the hostname and default gateway is set in /etc/sysconfig/network.

The following is an example:

```
NETWORKING=yes
NETWORKING_IPV6=yes
HOSTNAME=omegalx-pri
GATEWAY=10.100.1.254
```

Next the individual network interfaces are setup in the /etc/sysconfig/network-scripts directory. There will be a file for each ethernet interface (plus other miscellaneous scripts). The filename is in the form of ifcfg-*dev* where *dev* is the name of the device (i.e. eth0). Systems with more than one network interface will have additional files that start with ifcfg-. For example, ifcfg-eth1 or ifcfg-eth2.

The following is an example ifcfg-eth0:

```
# Intel Corporation 82541PI Gigabit Ethernet Controller
DEVICE=eth0
BOOTPROTO=static
HWADDR=00:1B:21:02:66:01
ONBOOT=yes
TYPE=Ethernet
IPADDR=10.100.1.215
NETMASK=255.255.255.0
```

DHCP is also supported and would look like the following:

```
# Intel Corporation 82541PI Gigabit Ethernet Controller
DEVICE=eth0
BOOTPROTO=dhcp
HWADDR=00:1B:21:02:66:01
ONBOOT=yes
TYPE=Ethernet
```

4.1.2   DNS server

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

```
search yourdomainname.com
nameserver 8.8.8.8
nameserver 8.8.4.4
```

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

4.1.3   Comtrol Devicemaster Serial Server

The Comtrol serial server configuration is in /etc/nslink.conf. The following is an example file:

```
bootfile-DM /etc/devmast.bin

10.100.1.203 32 30
10.100.1.204 32 30
```

The bootfile-DM line is the firmware file to upload to the Devicemaster device. There is a line for each of the Devicemasters the Omega connects to. In this case there are two 32 port Devicemasters using a 30 second timeout. A connection check is sent to each serial server every timeout/2 seconds. If more than timeout seconds pass between receiving connection check responses, the link will timeout and any open ports on that serial server will report errors. A value of 0 disables the link timeout.

Clustered systems need to use the same server key and certificate on both the primary and standby servers.

4.1.4 Digi Etherlite Serial Server

The Digi Etherlite serial server configuration is done with the command below. Replace the 1.2.3.4 with the IP address of the Digi Etherlite.

The DA in the command below is part of the device name. In this example the device names will be /dev/ttyDA00 to /dev/ttyDA31. If you use multiple Etherlite per system increment the A after the D to B. For example, DB then DC then DD, etc.

```
dgrp_cfg_node -v -v init DA 1.2.3.4 32
```

Clustered systems require the above step to be performed on both the primary and standby servers.

4.1.5 Kernel limits

Both Postgresql and Apache (mod_python) need the default kernel System V inter-process communication (IPC) values increased. Edit `/etc/sysctl.conf` and add the following to the end of the file:

```
# Controls the maximum size of a message, in bytes
kernel.msgmnb = 65536

# Controls the default maximum size of a mesage queue
kernel.msgmax = 65536

# Controls the maximum shared segment size, in bytes
kernel.shmmax = 68719476736

# Controls the maximum number of shared memory segments, in pages
kernel.shmall = 4294967296

# So we can increase Postgresql max connections - also apache mod_python
# SEMMSL - The maximum number of semaphores in a semaphore set
# SEMMNS - The maximum number of semaphores in the system
# SEMOPM - The maximum number of semaphores in a single semop call
# SEMMNI - The maximum number of semaphores sets
kernel.sem = 250 64000 23 1024
```

The shared memory settings above may have already been done so check the file (it isn't very large). The semaphore settings will typically always need to be added. After adding the above values run `sysctl -p` to have the values take effect immediately.

Clustered systems will require this change on both the primary and standby servers.

4.1.6   Database - Postgresql

> Important: Please check the Database Section below for information on customizing the createdb.sql script before creating the initial database.

From the /opt/omegalx directory type the following to create the OMEGA-LX database and load some initial data:

```
psql -U postgres -d omegalx -f db/createdb.sql
psql -U postgres -d omegalx -f db/data.sql
```

From the /opt/omegalx directory type the following to create the OMEGA-LX logging database:

```
psql -U postgres -d omegalog -f db/createlogdb.sql
```

From the /opt/omegalx directory type the following to create the OMEGA-LX thinclient database:

```
psql -U postgres -d thinclient -f db/createtcdb.sql
```

Clustered systems only require the above steps to be performed on the primary server.

4.1.7   Anti-spam - Spamassassin

The default spamassassin config file supplied by Hark should be good for most installations.

4.1.8 Web

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 normally 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 or Thawte 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 difficult to guess, but easy for you to remember because you will need it later in this process.

```
mkdir -p /opt/omegalx/ssl/gencert
cd /opt/omegalx/ssl/gencert
wget http://support.harktech.com/dl/omegalx/openssl.cnf
openssl genrsa -des3 -out server.key 4096
```

To create a self-signed certificate follow the steps below then perform the steps 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 -config openssl.cnf -extensions v3_req

  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. As we are creating a self-signed certificate that will only be used on this server we will use a very similiar Common Name as our server certificate uses. However the Common name must be different from the server certificate common name so we append a CA to the certificate common name. The -extensions v3_req is only needed if you are creating a multi-domain certificate. Make sure to edit the openssl.cnf and add your domains to the subjectAltName line. The openssl configuration program will not ask you for the domain names.

    - Enter pass phrase for ca.key:
    - Country Name (2 letter code) [US]:
    - State or Privince 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) []:omegalx.harktech.com CA

– Email Address []:support@harktech.com

Creating the certificate request. This is used for both self-signed and authority signed certificates. The challenge password and company name are both optional and you can just press <ENTER> to skip them.

- openssl req -new -key server.key -out server.csr -config openssl.cnf

  – Enter pass phrase for server.key:

  – Country Name (2 letter code) [US]:

  – State or Privince 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) []:omegalx.harktech.com

  – Email Address []:support@harktech.com

  – A challenge password []:

  – An optional company name []:

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 server.crt. For self-signed certificates the server.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.

Finally in order for apache to start automatically without user intervention save a non-secure version of the server key.

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

- cp -p server.pem server.crt ..

4.2 Database

The database design is stored in an SQL script in /opt/omegalx/db/createdb.sql. This script can be run when the system is first installed or if at any time you need to recreate the database from scratch. If you wish to change the default password for the database change it in the CREATE USER line near the beginning of the script. Also make sure to change the password in the database connection string in the omega.ini file.

There are also a few fields that you may want to modify. Keep in mind these modifications may be overwritten with future updates so you may want to copy createdb.sql to a different name and make your changes in that file. The following are some defaults you may wish to modify for your installation:

- idblock.timezoneoffset

- idblock.daylightsaving

- service.sendfields

- service.maxmessagelen

- service.maxlenperpage

- subscriber.timezoneoffset

- subscriber.daylightsaving

- virthost.sendfields

These defaults are only used if the field value is not specified when the record is created. Other fields may also be modified to suite your installation, but these are the most popular.

See the "Database" chapter for more information on the database design.

4.3 omega.ini

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

4.3.1   [common]

Common settings for all programs.

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. Up to two LICENSE_KEY lines may be specified. This is to support a clustered 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.

CHECK_SOURCE	Enable subscriber source overrides. This allows subscribers to specify which sources they wish to receive messages from. This can be GCP, HTTP, SMPP, SMTP, SNPP, TAP, TNPP, or WCTP.
SERVER_NUM	Specify which of the load-balanced servers this server is. This is used to keep the messageid unique across machines in the load balance array. Allowable values are 1 to 8. If this value is changed the service will need to be restarted.
DB_CONN_1	This field specifies the postgresql connection string. As of version 5.0 we support multiple database connections. DB_CONN_1 must be a valid database connection string as all activity will go over this connection. In addition, for geo-redundancy, we support DB_CONN_2 through DB_CONN_8 for copying messages only.
DB_CONN_2	This field specifies an additional database connection that all message transactions will be copied to for geo-redundancy. This will allow a 2-way message status to be checked from any server in the group.
LOG_DB_CONN	This field specifies the connection string for logging. This allows the billing logs to be written to a PostgreSQL database. Billing logs will still be written to the flat file. To turn off the flat file logs and only write to the billing log database set LOG_PERIOD to NONE (or 0).
TC_DB_CONN	This field specifies the connection string for the thin client database. The Omega-LX supports writing to and reading from a special thin client SQL database for sending and receiving messages via a special thin client application running on a smartphone.

EMAIL_SUBJECT	The subject to use for outgoing emails if there is no subject on the incoming message.
SMARTHOST_URL	This is a URL formatted string that describes how to connect to a mailserver that can send email to the Internet. This can be the local Postfix server (127.0.0.1:25) or a corporate email server. This is used to send countdown notification emails and also SMPP replies or other outgoing SMTP requests. This field is in the format of smtp://user:pass@server:port#inittime:sectime. The server and port are required. The user:pass@ and #inittime:sectime are optional. A future release will support using the user:pass for sending to an SMTP server that requires authentication. If #inittime:sectime are not specified, 30000 and 2000 will be used. Examples: `smtp://1.2.3.4:25` or `smtp://myuser:mypass@1.2.3.4:25#30000:2000`.
MCR_RESPONSE_DOMAIN	The domain name to use for email rerurn address of Multiple Choice Response (MCR) from the two-way paging gateway.
AUTO_CONFIRM_RECEIPT	Set the confirm_page_delivery flag when sending a WCTP message out to the GL-3200.
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/or TNPP port threads. The maximum value currently allowed in the OMEGA-LX 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.

STRIP_IDDASH	Strip any dashes sender may have included in the pager ID.
STRIP_PLUSONE	Strip the +1 from an 11-digit number starting with 1.
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.

USE_OPAGE

Instead of immediately sending the incoming messages to the outgoing service and sending the real-time response, the messages are acknowledged and stored in the pageque table. The pageque table is then scanned by the opage program and delivered to their destination.

DROP_PRIVILEGES

Drop super-user privileges and run as a non-privileged user soon after starting up.

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.

COUNTDOWN_NOTIFY

Specify an email address to send alerts to when a subscriber has reached their countdown limit. This is typically used to notify a customer service rep so they will know why the subscriber's messages are not going through. The format of the message for the daily countdown type is "Subscriber xyz is disabled until midnight". For monthly countdown type it is "Subscriber xyz is disabled until 12am mm/01".

COUNTDOWN_NUMERIC

Contains the numeric message to send to the subscriber's pager when their countdown limit has been exceeded. This can be a customer service number followed by a code the caller can give so they know what the call is regarding. COUNTDOWN_NOTIFY must also be set for this feature to work. Up to 32 digits may be specified.

COUNTDOWN_ALPHA

Contains the alpha message to send to the subscriber's pager when their countdown limit has been exceeded. COUNTDOWN_NOTIFY must also be set for this feature to work. Up to 120 characters can be specified.

IPFILT_NOTIFY

Specify an email address to send alerts to when a message is blocked due to an IP filter.

THROTTLE_NOTIFY

Specify an email address to send alerts to when a message is blocked due to subscriber input throttle filter.

REPLYABLE_HEADER

The email header to send if this message came from a protocol that is replyable for two-way paging. If this field is set and the subscriber is two-way and the message came in via SMTP or WCTP and it is delivered via SMTP a replyable header such as `X-Replyable: Yes` will be added to the outgoing email. Otherwise `X-Replyable: No` will be added.

AUTO_UPDATE_DATABASE

Set this field to Y to allow the Omega-LX to automatically update the database schema during a software update if needed. Setting to N is not recommended as it means that database schema updates will need to be performed manually.

LOG_PERIOD

The amount of time to write to a billing log file. This is typically set to DAILY to create a new billing log each day. Other allowable values are WEEKLY, MONTHLY, and ONEDIR. WEEKLY will create a new billing log every seven days of the month. At the end of the month a new weekly file will be created for the next month even if there are not exactly 28 days in a month. MONTHLY will create a new billing log each month. ONEDIR will create a single level directory for the debug logs for that date. In other words in the log directory there will be one directory per date in the format of YYYY-MM-DD and all the billing logs for the various protocols will be contained within. As of version 5.0 if there is a LOG_DB_CONN defined and reachable, the billing logs will be written to the database. If you only want the logs to go to the database and not written to flat files set LOG_PERIOD to NONE.

LOG_COMPRESS	Compress billing logs. On busy systems the billing logs can take a large amount of space. This option allows the text files to be compressed with gzip. The available values are NONE, REALTIME, and DELAY. We recommend using DELAY as this will cause the files for the previous day to be zipped. This is more efficient from a CPU usage and for file fragmentation.
ID_FORWARD	This is a special prefix that allows incoming SMPP messages from a handset to be delivered to the email address specified in the beginning of the message.
REPLY_FORWARD	This is a special prefix that allows replies to messages sent to SMPP to be received and sent to the original sender via email.
RANDOM_DEV	The device to use for a random number generator. This is typically PRNG.
MAX_RANDOM_DIGITS	The maximum number of digits to pull from the random device (such as /dev/random or /dev/urandom) at a time. This can be from 2 to 19 digits.
FORCE_SUBMAXMSGLEN	Enforce the subscriber maximum message length on outgoing messages that include message headers in the outgoing message. For example, if the subscriber max message len is 240 and they receive and email, the email headers may be added to the message increasing the length past 240 characters. With the option set, the length of that message will be trimmed to 240 characters.

4.3.2   [gcpd]

Glenayre Computer Protocol server configuration.

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

AFFINITY_MASK	Processor affinity mask for multiple processor (SMP) machines. Typically this is set to 0 to run on any of the processors in the system. This value does not need to be changed unless you wish to reserve certain processor or processor cores for dedicated programs.
MAX_THREADS	The maximum number of simultaneous threads to allow this program to create. One thread is required for each port/connection.
STORE_MESSAGES	If this value is set to YES or 1 messages will be stored in the message table. Otherwise they will be paged out, but not store in message. This option must be enabled (set to YES or 1) if the USE_OPAGE option in [Common] is enabled.
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.
MODIFY_DNE_CREATE	Allow automatic creation of subscriber and pager records if modify requests a non-existant record. The default value is N to not automatically create non-existant records.

4.3.3 [httpd]

Omega HTTP server.

DEBUG_LEVEL	Level of debugging information to write to the debug directory.
AFFINITY_MASK	Processor affinity mask for multiple processor (SMP) machines. Typically this is set to 0 to run on any of the processors in the system. This value does not need to be changed unless you wish to reserve certain processor or processor cores for dedicated programs.
MAX_THREADS	The maximum number of simultaneous threads to allow this program to create. One thread is required for each port/connection.
STORE_MESSAGES	If this value is set to YES or 1 messages will be stored in the message table. Otherwise they will be paged out, but not store in message. This option must be enabled (set to YES or 1) if the USE_OPAGE option in [Common] is enabled.
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 65536 can also be entered as 64k.
SESSION_EXPIRE	The amount of time in minutes before the HTTP session times out.
CAPTCHA_FONT	The font used to draw the captcha text. See the httpd section in the "Program Descriptions" chapter for more information.
CAPTCHA_WIDTH	The width in pixels of the graphical image displayed to the web user.
CAPTCHA_HEIGHT	The height in pixels of the graphical image displayed to the web user.

CAPTCHA_QUALITY   The relative quality of the captcha image.

4.3.4 [isid]

Omega ISI server. Allows connection of multiple remote Hark ISI boxes to this location.

DEBUG_LEVEL   Level of debugging information to write to the debug directory.

AFFINITY_MASK   Processor affinity mask for multiple processor (SMP) machines. Typically this is set to 0 to run on any of the processors in the system. This value does not need to be changed unless you wish to reserve certain processor or processor cores for dedicated programs.

MAX_THREADS   The maximum number of simultaneous threads to allow this program to create. One thread is required for each port/connection.

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 65536 can also be entered as 64k.

4.3.5 [monitor]

System resource monitor.

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. See DEBUG_LEVEL in the [gcpd] section for a list of values.
SCAN_INTERVAL	The amount of time between scans. Typically 60 seconds.
MONITOR_HD	Monitor hard drive disk usage.
MONITOR_MEM	Monitor memory usage. This is of limited usefulness in Linux as Linux will use free memory for caching and buffers. If enabled you may receive many alarms about low-memory even when the system has plenty of memory available that can be reclaimed from the cache and buffer space.
DRIVES	The filesystem to monitor. Typically /opt/omegalx.
MEM_NOTICE_MIN	A notice is sent if available memory drops below this value.
MEM_WARNING_MIN	A warning is sent if available memory drops below this value.
MEM_ERROR_MIN	An error is sent if available memory drops below this value.
HD_NOTICE_MIN	A notice is sent if available drive space drops below this value.
HD_WARNING_MIN	A warning is sent if available drive space drops below this value.
HD_ERROR_MIN	An error is sent if available drive space drops below this value.
FUTURE_INTERVAL	The amount of time in seconds between scans of the message database to process future delivery messages. Set to 0 to disable future message scanning. When a central database server, rather than a local database, is used only one server should be set to scan for future delivery messages. If for some reason you need to take the server set to scan the future messages out of the load-balance rotation you can set the FUTURE_INTERVAL on that machine to 0 and the FUTURE_INTERVAL on another machine in the array to take over future

CLEANUP_INTERVAL   The amount of time in minutes between scans of the message database to remove expired messages. The message cleaning should also only be performed on one server in the array. The same rules apply as for FUTURE_INTERVAL. Set this value to 0 to disable message purging and set it greater than zero on one of the other machines in the load-balanced array to take over old message purging.

VACUUM_TIME   The time of day in 24 hour time (from 0000 to 2359) to vacuum the database. Vacuums are scans of the database marking expired data and index entries available for future reuse. Vacuuming the database is something that should be done at least once per day (more often for busier machines). This function should also only be performed by one server in the load-balanced array. Set to -1 to prevent this server from vacuuming the database. Make sure one of the machines in the array is set to vacuum the database at least once per day. In the version of Postgresql currently being used the default is to auto-vacuum. If you are using the default Postgresql auto-vacuum set this field to -1 so the monitor program doesn't attempt to vacuum also.

COUNTDOWN_RESETTIME	The time of day in 24 hour time (0000 to 2359) to reset the subscriber countdown values. This is typically 0000 to reset subscribers at midnight.
SCHEDULE_INTERVAL	The amount of time in seconds between scans of the schedule table for messages that need to be delivered.
MESSAGE_RETENTION	The amount of time in minutes to store messages.
PURGE_DEBUG_DAYS	The number of days to retain debug logs.
PURGE_DEBUG_HOUR	The hour of the day to purge debug. This is typically 3 for 3 am. Valid values are 0 to 23.
PURGE_ERROR_DAYS	The number of days to retain the error logs in /var/opt/omegalx/error/YYYY/MM.
TESTPAGE_ID	A valid pager ID to send test messages to for system monitoring.
TESTPAGE_INTERVAL	The interval in minutes between test pages.
COMPRESS_LOG_DAYS	The number of days to wait before compressing the plain text billing logs with gzip.
COMPRESS_LOG_HOUR	The hour of day in 24 hour time (0000 to 2359) to run the billing log compressor.
PRIMARY_PING	The IP address of the primary server. The monitor application will ping the primary IP address and if it fails, send an alarm.
STANDBY_PING	The IP address of the standby server. The monitor application will ping the standby IP address and if it fails, send an alarm.
PSMON_PORT	The name of the serial port with the power supply monitor hardware installed. This is typically a /dev/ttyUSB... port. The power supply monitor takes a two-wire input and if a short is detected sends an alarm. If a power supply module fails the alarm can be sent so that a remote system will alert someone to replace the module restoring redundant operation.

4.3.6 [onixd]

Main process starter/monitor.

DEBUG_LEVEL	Level of debugging information to write to the debug directory.
SHUTDOWN_TIME	The amount of time in seconds to wait for processes to gracefully exit before forcing them to exit.
START	Programs to start and monitor. This is a comma separated list of program names.

4.3.7 [opage]

Omega outgoing paging server.

DEBUG_LEVEL	Level of debugging information to write to the debug directory.
AFFINITY_MASK	Processor affinity mask for multiple processor (SMP) machines. Typically this is set to 0 to run on any of the processors in the system. This value does not need to be changed unless you wish to reserve certain processor or processor cores for dedicated programs.
MAX_THREADS	The maximum number of simultaneous threads to allow this program to create. One thread is required for each port/connection.
MAX_QUEUE_ENTRIES	Maximum number of pages to keep in the processing queue at a time.
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.

SCAN_TIME	The amount of time between scans. Typically 5 seconds.
POOL_THREADS	The number of threads to create to process pageque records. This is typically set to 10.

4.3.8   [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.

4.3.9   [smppd]

Omega SMPP server.

DEBUG_LEVEL	Level of debugging information to write to the debug directory.
AFFINITY_MASK	Processor affinity mask for multiple processor (SMP) machines. Typically this is set to 0 to run on any of the processors in the system. This value does not need to be changed unless you wish to reserve certain processor or processor cores for dedicated programs.

MAX_THREADS	The maximum number of simultaneous threads to allow this program to create. One thread is required for each port/connection.
MAX_QUEUE_ENTRIES	Maximum number of pages to keep in the processing queue at a time.
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.
STORE_MESSAGES	If this value is set to YES or 1 messages will be stored in the message table. Otherwise they will be paged out, but not store in message. This option must be enabled (set to YES or 1) if the USE_OPAGE option in [Common] is enabled.
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.
QUEUE_TIMEOUT	The amount of time in milliseconds to wait for a response from the remote SMPP server before returning a packet timeout to the client.

4.3.10   [smtpd]

Omega SMTP server.

DEBUG_LEVEL	Level of debugging information to write to the debug directory.
AFFINITY_MASK	Processor affinity mask for multiple processor (SMP) machines. Typically this is set to 0 to run on any of the processors in the system. This value does not need to be changed unless you wish to reserve certain processor or processor cores for dedicated programs.
MAX_THREADS	The maximum number of simultaneous threads to allow this program to create. One thread is required for each port/connection.
MCR_RESPONSE_HEAD	Allows the definition of a message prefix the remote server may send with responses. If this field is defined and the message response starts with this value it will be stripped from the beginning of the message. An example of this the the GL-3200 which prefixes its mcr responses with "Response:".
MCR_RESPONSE_TAIL	Allows the definition of a trailing part of the message to trim. This text and any text after it in the message response will be trimmed. An example is the GL-3200 which appends "Your message" and the original message.

TWOWAY_CONFIRM_HEAD

Allows the definition of a message prefix the remote server may send with twoway page confirmations. If this field is defined and the message response starts with this value it will be stripped from the beginning of the message. An example of this the the GL-3200 which prefixes its twoway confirmation with "Your message was delivered to".

KEEP_TMPFILE	For troubleshooting purposes only. Should be set to N normally.
THROTTLE_CODE	The code to send back to SMTP client when the message is throttled due to the traffic rate being exceeded. The default is 451.

STORE_MESSAGES	If this value is set to YES or 1 messages will be stored in the message table. Otherwise they will be paged out, but not store in message. This option must be enabled (set to YES or 1) if the USE_OPAGE option in [Common] is enabled.
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.

4.3.11 [snppd]

Omega SNPP server.

DEBUG_LEVEL	Level of debugging information to write to the debug directory.
AFFINITY_MASK	Processor affinity mask for multiple processor (SMP) machines. Typically this is set to 0 to run on any of the processors in the system. This value does not need to be changed unless you wish to reserve certain processor or processor cores for dedicated programs.
MAX_THREADS	The maximum number of simultaneous threads to allow this program to create. One thread is required for each port/connection.
STORE_MESSAGES	If this value is set to YES or 1 messages will be stored in the message table. Otherwise they will be paged out, but not store in message. This option must be enabled (set to YES or 1) if the USE_OPAGE option in [Common] is enabled.

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.

4.3.12   [syspage]

Syspage is responsible for receiving the alarms from the various Omega-LX compo-
nents and sending them based on the entries in the alarm table.

DEBUG_LEVEL   Level of debugging information to write to the
                        debug directory.

AFFINITY_MASK   Processor affinity mask for multiple processor
                        (SMP) machines. Typically this is set to 0 to
                        run on any of the processors in the system. This
                        value does not need to be changed unless you wish
                        to reserve certain processor or processor cores for
                        dedicated programs.

MAX_THREADS   The maximum number of simultaneous threads
                        to allow this program to create. One thread is
                        required for each port/connection.

LISTEN_PORT   The TCP port to listen for alarms on.

IGNORE_TIME   The amount of time in seconds after which to
                        ignore a stale alarm. This prevents sending alarms
                        that may have been delayed due to a back log of
                        alarms.

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.

SNMP_OID

The base SNMP OID string for sending alarms via SNMP.

4.3.13 [tapd]

Omega TAP server.

DEBUG_LEVEL

Level of debugging information to write to the debug directory.

AFFINITY_MASK

Processor affinity mask for multiple processor (SMP) machines. Typically this is set to 0 to run on any of the processors in the system. This value does not need to be changed unless you wish to reserve certain processor or processor cores for dedicated programs.

MAX_THREADS

The maximum number of simultaneous threads to allow this program to create. One thread is required for each port/connection.

STORE_MESSAGES

If this value is set to YES or 1 messages will be stored in the message table. Otherwise they will be paged out, but not store in message. This option must be enabled (set to YES or 1) if the USE_OPAGE option in [Common] is enabled.

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.

4.3.14   [thinclient]

Omega thin client application server.

DEBUG_LEVEL	Level of debugging information to write to the debug directory.
AFFINITY_MASK	Processor affinity mask for multiple processor (SMP) machines. Typically this is set to 0 to run on any of the processors in the system. This value does not need to be changed unless you wish to reserve certain processor or processor cores for dedicated programs.
MAX_THREADS	The maximum number of simultaneous threads to allow this program to create. One thread is required for each port/connection.
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.
SCAN_TIME	The amount of time between scans. Typically 5 seconds.

4.3.15   [tnppd]

Omega TNPP server.

DEBUG_LEVEL	Level of debugging information to write to the debug directory.
AFFINITY_MASK	Processor affinity mask for multiple processor (SMP) machines. Typically this is set to 0 to run on any of the processors in the system. This value does not need to be changed unless you wish to reserve certain processor or processor cores for dedicated programs.
MAX_THREADS	The maximum number of simultaneous threads to allow this program to create. One thread is required for each port/connection.
MAX_QUEUE_ENTRIES	Maximum number of pages to keep in the processing queue at a time.

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.

DUP_ARRAY_SIZE

The maximum number of entries in the duplicate checking array. This can potentially take a large amount of memory with large TNPP packet sizes. Changes to this field will only take affect after restarting the tnppd program.

DUP_CHECK_TIME

The amount of time in seconds to check for duplicate packets in the duplicate checking array. The default is 300 seconds (5 minutes). Set this field to 0 to disable duplicate message dropping. This field can be modified without needing a restart.

STORE_MESSAGES

If this value is set to YES or 1 messages will be stored in the message table. Otherwise they will be paged out, but not store in message. This option must be enabled (set to YES or 1) if the USE_OPAGE option in [Common] is enabled.

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.

4.3.16 [wctpd]

Wireless Communications Transfer Protocol server.

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. See DEBUG_LEVEL in the [gcpd] section for a list of values.
AFFINITY_MASK	Processor affinity mask for multiple processor (SMP) machines. Typically this is set to 0 to run on any of the processors in the system. This value does not need to be changed unless you wish to reserve certain processor or processor cores for dedicated programs.
MAX_THREADS	The maximum number of simultaneous threads to allow this program to create. One thread is required for each port/connection.
STORE_MESSAGES	If this value is set to YES or 1 messages will be stored in the message table. Otherwise they will be paged out, but not store in message. This option must be enabled (set to YES or 1) if the USE_OPAGE option in [Common] is enabled.
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 65536 can also be entered as 64k.

4.4   Example omega.ini

See /opt/omegalx/omega.ini.

Chapter 5

Database Maintenance

There are three methods to maintain the Omega internal databases. These are Command Line, Web-based, and Computer Interface. The command line interface is useful for modifying database entries from over an SSH connection. The web-based interface provides and easy to use interface accessible from any modern browser that supports Javascript and Cascading Style Sheets (CSS). In order to view real-time stats through the web interface a browser that supports AJAX is required. Finally there is also a computer interface for programming the databases over a TCP/IP connection from a corporate billing system.

5.1   Command line

The OMEGA-LX database can be maintained using a standard SQL interface. To login to the database type `psql -U postgres -d omegalx`. The database definition is stored in db/createdb.sql. See the postgresql section for more information.

5.2   Web browser based

The web-based administrative interface allows a user to modify subscribers and the majority of the system settings from any standard web browser on the TCP/IP network. There is also a limited set of pages available for subscribers to maintain their own information.

5.2.1   Subscriber access

http://localhost is used for accessing the web pages the subscriber has access to. An existing login and passcode is needed to access this web page.

Once logged in you will have the following options:

- Subscriber - Allows access to subscribers, subscriber pagers, email filters, and other subscriber settings.

- System - Accessible only to users with a high enough security level. All system setup and configuration is done from these menu selections. This is where the devices, output groups, dialing types, classes of service and other system settings are maintained.

- Stats - Display real-time statistics for each of the programs. This allows you to view which Omega applications are running and also click on those programs to view the status of the individual threads in each program that supports it.

- Logout - Logout of this session. This is only required if you want to switch from the admin web pages to the subscriber web pages described below.

There is now the capability for resellers to access their own accounts. Setup a username for the reseller with the reseller security level and they will only be able to view mailboxes with the same account number as the account number defined in the reseller's webuser record.

5.2.2   Customization

The web pages are written in standard HTML with tags that are replaced when the page is requested. These pages can be modified to suite your needs. It is not recommended to change the admin web pages. They are very specific to the version of the Omega and may be overwritten during a software update. The admin web pages are for your internal use and reseller access only. Subscriber's will not see them. Subscriber web pages however can be freely modified. The recommended method for customizing the subscriber web pages is to make a copy of everything in the the /opt/omegalx/www/default directory except the admin sub-directory into another directory such as /opt/omegalx/www/custom1 (feel free to name custom1 to any legal filename). The directory you specify will need to be added to virthost so the server knows which sub-directory to use. In the above example the directory field in the virthost record would be custom1 (the /opt/omegalx/www part is already assumed). Now that you have a copy of the default directory in the custom1 directory you may edit the web pages and cascading style sheets to your liking.

5.3   Computer Interface

The OMEGA-LX can be programmed using the Glenayre Computer Protocol for compatibility with most billing systems available. GCP versions 6.0, 6.1, and 8.0 are supported.

See the gcpd section in "Protocol Servers" for more information on configuring

and using GCP.

5.3.1 GCP Commands

The following GCP commands are supported:

Command	Function
@RV	Read Version
@SN	Set Node (command accepted but ignored)
@LV	Login (uses username/password from subaccess)
@PO	Page Out
@CR	Create Record
@RE	Read Record
@DR	Delete Record
@MR	Modify Record
@QT	Quit (Hark extension)
@RK	Send rekey command to pager (Hark extension GCP 9+)
@CD	Send clear device command to pager (Hark extension GCP 9+)
@GK	Generate random key (Hark extension GCP 9+)

The following table shows the mapping of Glenayre fields to the Omega-LX database:

Number	GCP description	Database field
1	customer number	subscriber.subscriberid, pager.subscriberid
2	capcode	pager.idcap,pagertypepagerfunction,tnpppackettype
3	account number	subscriber.accountnumber
4	service type	pager.pagerclass (support 01, 02, 03, 04, 09)
5	coverage region	pager.outputgroup
6	access code	subscriber.password
9	answer type	subscriber.answertype
14	priority	pager.pagerpriority
20	date created	subscriber.datecreated
21	date altered	subscriber.datealtered
23	call count	subscriber.callcount
35	ext group	subscriber.groupmember1 to groupmember16
36	valid	subscriber.enabled
41	language	subscriber.language
43	callerpasscode	subscriber.callerpass
45	max datapage len	subscriber.maxmessagelen (mapped through gcpdatal
70	16 digit customer number	subscriber.subscriberid, pager.subscriberid
74	maildrop	pager.pagerclass (non-zero=class 6, zero=class A)
78	16 digit ext group	subscriber.groupmember1 to groupmember16
122	date created (4 digit year)	subscriber.datecreated
123	date altered (4 digit year)	subscriber.datealtered

GCP version 9

GCP version 9 isn't an actual Glenayre version. It is used to allow additional fields for programming the encryption keys in the encryptionkey table.

Chapter 6

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.

6.1   service

All outgoing delivery types must be defined in the service table. This table contains the settings needed to send messages via the various protocols. For example, to send messages via SNPP to snpp.example.org, a service will be setup with a remote host of snpp.example.org with a port number of 444. The service table also contains the definitions for all serial ports whether incoming or outgoing. See the service description in the database chapter for more information. In addition a service needs to be created for each network server (i.e. HTTP, SMTP, SNPP, and WCTP). The Omega-LX actually supports running a protocol, such as SNPP, on more than one port. This can be done if you need to support different options or want to restrict certain access. The service table also contains the configuration for any local serial ports.

6.1.1   Fields

servicenum   A unique identifier for the service.

name   A descriptive name for service.

porttype   The type of port. 1=serial, 2=network.

portstatus   The port status. 0=off-line, 1=on-line, 2=fault-off

backupservice   The service number to use if this service fails.

direction   The direction of this port. Allowable values are
                             IN, OUT, or BOTH. These must be entered in
                             upper-case.

protocol   The following protocols are supported: GCP,
                             HTTP, SMPP, SMTP, SNPP, TAP, TNPP, and
                             WCTP.

protocoloption   Bit-mask of options for this protocol. Add together
                             the values of the options you wish to enable.

SMTP protocol options:

32   0x00000020   Enable subject switches

SNPP protocol options:

        1   0x00000001   Strip CRLF on incoming DATA connection
134217728   0x08000000   Require login to send a message

WCTP protocol options:

134217728   0x08000000   Require login to send a message

packetsize   The size of the data packet. TAP is typically 256,
                             TNPP may be 1024 or 4096. These are the only
                             allowable values. This field is not used for other
                             protocols.

buffsize   The size of the internal read buffer. This is typi-
                             cally 8192. Network servers may use larger values.
                             Recommended values for HTTP and WCTP are
                             16384.

maxfromlen   Maximum number of characters of the From: email
                             address to send to the notification device. Allow-
                             able values are 0 to not limit the from length or a
                             number from 1 to 80.

maxsubjectlen   Maximum number of characters of the Subject: email header to send to the notification device. Allowable values are 0 to not limit the from length or a number from 1 to 80.

sendfields   Specify which email headers to send out. Allowable values are F, S, B, C, T, D, and N. 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

headerfields   Specify which email headers the output device supports as headers. Allowable values are F, S, D, and T. These may be combined. For example to send from and subject use FS.

F	From
S	Subject
T	Timestamp
D	Disposition-Notification-To

prefixtext   Text to prepend to the outgoing message. This may be up to 16 characters and will be the first thing sent to the notification device.

suffixtext   Text to append to the outgoing message. This may be up to 16 characters and will be the last thing sent to the notification device.

maxmessagelen   The maximum length of message to accept for incoming services. Also, the maximum length of the message to send to a remote server.

maxlenperpage

The maximum length of message to send in a single message. If the maxlenperpage is less than the maxmessagelen for a remote service, the message will be split into multiple messages for sending.

overlenservice

If the maxmessagelen and the maxlenperpage are set to the same value and the message length exceeds this value and this field is set to a valid service, the message will be sent using the service specified in this field instead of the original service.

username

An optional username to login as if the remote service requires it.

password

The password to use for the above username.

inputrate

The maximum number of packets to accept in one minute. This is used to implement a "soft" throttling method. As of 4.2-5 this is now supported for HTTP, SMPP, SMTP, SNPP, TNPP, and WCTP.

outputrate

The maximum number of packets to send in one minute. This is used to prevent flooding a slower output device. This is currently only supported in SMPP, TNPP, and opage output threads.

maxthreads

The maximum number of threads to allow for the service.

maxrecipients

The maximum number of recipients to allow per session.

idappend

string to append to the end of the outgoing email address. This is for appending the domain name to the end of the outgoing id.

idformat

Specify format of incoming ID. This is to allow a specific incoming service to modify the incoming ID before it is passed to the ID lookup routines. For example, a specific incoming TNPP connection may only send 8 digits (older Glenayres) while the outgoing service requires 10 digits. A format of 843%7i can be used to automatically prefix the 843 area code to the ougoing pager id.

erroraction	The action to take for error messages. 0=ignore errors, 1=log errors to the errors directory, 2=notify errors using syspage, and 3=log and notify.
logtype	The type of connections to write to the billing logs. 0=none, 1=input records, 2=output records, 3=both input and output.
balancegroup	SMPP load balancing group. The smpproute will specify the group to use. Outgoing packets for the smpproute will be load balanced across the services in the same group. The packet will be sent to the least active service.
allowidblock	Specify whether this service allows idblock lookups for incoming messages. It may be desirable to have certain incoming services only allow messages to numbers that can be looked up in subscriber or LDAP and not let the default fall-through go to the idblock number ranges.

Serial port services support the following additional fields:

comport	The name of the RS-232 port to use for RS-232 connections. For example, /dev/ttyUSB0 or /dev/ttySI28. Maximum length is 32 characters.
modemtype	The modemnum from the modemtype table. This field may be set to 0 to indicate a direct RS-232 connection.
modemnumber	Modem number to dial for outgoing connections. Leave blank for direct RS-232 connections.
baud	Specifies the baud rate of the RS-232 connection
parity	Parity of the RS-232 connection. May be E for Even, O for Odd, M for Mark, S for Space, or N for None.

databits   Number of data bits. May be 7 or 8.

stopbits   Number of stop bits. May be 1 or 2.

TCP/IP services support the following fields:

sockdomain   This field should always be set to INET for network connections.

socktype   This field should be set to TCP for TCP/IP connections or UDP for UDP connections.

sockaddr   Typically this field will be set to 0.0.0.0 which specifies that the outgoing connection will not be sent out using a particular IP address. If your system has multiple ethernet interfaces for example a public Internet and private VPN connection, you may specify a valid IP address for the connection you wish to use to force the outgoing connection to that interface. For incoming (i.e. server) connections this specifies the IP address to bind to.

sockport   Typically this field will be set to 0 which allows outgoing connections to come from a specific port. This field is not used for incoming (i.e. server) connections.

remotehost   The Internet host name of the remote server. This may also be an IP address instead of the host name. Leave this field blank to act as a server connection (i.e. Listen for incoming connection requests).

remoteport   The TCP port number of the remote server. This is a number in the range of 1 to 65535. This field also specifies the port number to listen on for server connections.

encrypt   Encrypt the network connection using a symmetric encryption. This supports recieving encrypted network connections from other Hark devices such as the ISI and TNPP-LX, or other OMEGA-LX servers.

inittime	The initial read timeout in milliseconds.
sectime	The amount of time in milliseconds to wait for additional data once something has been read.
filternum	The ipfilt filter number to use for "hard" throttling.
keepopentime	The amount of time in seconds to keep a connection open waiting for additional data. If this value is less than the inittimeout the connection will wait for inittimeout.
hellomessage	Initial prompt to send on incoming SMTP and SNPP connections. The OMEGA-LX software version can be sent with %v. For example, Hark OMEGA-LX v%v SMTP Ready or Hark OMEGA-LX v%v SNPP Ready.

GCP services support the following additional fields:

gcpversion	The GCP version to support for this service. Allowable values are 6.000, 6.100, and 8.000.

HTTP services support the following additional fields:

httptype	The type of HTTP server we are connecting to. 0=default, 1=GL3200.
httpiddashes	Insert dashes into the 10-digit number being sent. The default value is FALSE.
httppost	Use POST method to send message, otherwise use GET. The default value is TRUE (use POST).
httpsendformname	The full URL of the HTTP form to POST the message to for delivery using the carrier's web site. This and the other HTTP paging fields are mostly used by cellular phone providers which only offer an email gateway for paging via the Internet. Direct HTTP is preferable to SMTP because you get an immediate acknowledgement if the message was accepted or not. With email you may not ever know if the message was actually accepted and you have no control over the format of the message (for example which email headers are sent).

httpidname	The name of the HTTP form field that accepts the pager or cellular phone number to page.
httpsendmsgname	The name of the HTTP form field that accepts the message.
httpsuccessstring	The text (or portion of) that specifies the message was accepted for delivery.
httpfromname	The name of the HTTP form field that accepts the from address. This field is optional and if left blank the from address will not be sent. Also note that not all carriers support sending the from address.
httpsubjectname	The name of the HTTP form field that accepts the subject. This field is optional and if left blank the subject will not be sent. Also note that not all carriers support sending the subject.
httpextra	Additional text that needs to be posted to the HTTP form in order for the message to be accepted. This is used for special cases and the assistance of Hark technical support may be needed for proper setup.
httpmsglenname	The name of the HTTP form field that accepts the length of the message. This field is optional and if left blank the length will not be sent. Also note that not all carriers support sending the length.

SMPP services support the following additional fields:

sourceton	The source Type Of Number (TON) to use.
sourcenpi	The source Numbering Plan Indicator (NPI) to use.
destton	The destination Type Of Number (TON) to use.

destnpi	The destination Numbering Plan Indicator (NPI) to use.
systemtype	SMPP system type.
smppversion	The SMPP protocol version. Version 51 (0x33 for SMPP 3.3) and version 52 (0x34 for SMPP 3.4) are supported. One difference is SMPP 3.3 only supports 160 character messages, while SMPP 3.4 supports 254 character messages (or longer if TLV's are used).
datacoding	The data coding value to use. The default value is 3.
servicetype	The SMPP service type to use.
tnri	No response idle timer. The amount of time in milliseconds to wait after sending a packet for the response.
tnre	No response enquire link timer. The amount of time in milliseconds to wait for the enquire link response.
tidle	If there is no activity on this port in tidle milliseconds an enquire link is sent.

SMTP services support the following additional fields:

maxsize	The maximum size of email to accept. This value is advertised for ESMTP connections and enforced for both SMTP and ESMTP connections.
mdnheader	The value to use for the outgoing Message Disposition Notification Header if SENDFIELDS_MDN is enabled. The default value is Disposition-Notification-To. RFC2298 specifies Disposition-Notification-To, while Microsoft uses Return-Receipt-To. You may use one or the other.

noolderthan   Allows blocking of email with a Date: header older
                                    than this value in minutes. Set to 0 to disable
                                    older than checking.

nonewerthan   Allows blocking of email with a Date: header newer
                                    than this value in minutes. Set to 0 to disable
                                    newer than checking.

TAP services support the following additional fields:

extblock   Enable support for extended TAP blocks. The
                                    default value is TRUE.

transchar   Enable support for TAP transparency character
                                    insertion. The default value is TRUE.

respcode   Enable support for TAP v1.6+ response codes.
                                    These are 3 digit numbers which precede the re-
                                    sponse messages. The default value is true.

netevenparity   Force even parity for network connections. This is
                                    used when a terminal server provides the incoming
                                    modem access and the messages are sent to the
                                    Omega over a network connection.

tapprofilenum   Allow specification of a tap profile to set different
                                    timeout and counters. Also see tappassword for a
                                    way to set timeouts based on the TAP password
                                    used.

TNPP services support the following additional fields:

tnppsource   TNPP source ID to use when sending messages.

tnppdest   TNPP destination ID to use when sending mes-
                                    sages.

tnpptype   0=Normal, 1=Hark ISI, 2=CommOne, 3=RTS
                                    ATNP. Specifies any system specific variations of
                                    the TNPP protocol. For example, the ISI has spe-
                                    cial link tests to test the link status independently
                                    from the TNPP link test, CommOne has user-
                                    name/password and other protocol changes, and
                                    RTS ATNP also has a modified TNPP protocol.

inertia   Maximum number of TNPP "hops" to allow.

transcrc   Enable transparent CRC. The default is false which
                                 uses normal CRC. Normal CRC is a two-byte bi-
                                 nary value which is checked to make sure the packet
                                 has been received without corruption. Some sys-
                                 tems, such as those going through statistical mul-
                                 tiplexers, require the data to not include certain
                                 binary characters so transparent CRC splits the
                                 binary CRC into 4 printable characters. For ex-
                                 ample, a CRC of [5C][1B] would be split into the
                                 four printable characters '5C1B'.

simplex   Enable simplex connection. Simplex connections
                                 are also referred to as one-way or satellite connec-
                                 tions. These connections do not send ACK's or
                                 other responses to incoming packets, nor does it
                                 expect them on outgoing packets. See also sim-
                                 plextransmits.

acceptall   Consider all incoming TNPP packets for us. This
                                 means that any incoming packet will have the
                                 pager ID looked up in the database and delivered
                                 based on those settings. If this field is set to false,
                                 packets will be routed normally. If the packet
                                 destination node ID is the same as the service
                                 tnppsource the packet will be processed based on
                                 the database lookup, otherwise it will be routed
                                 based on the destination node ID in the tnpproute
                                 table.

requirelinkresp   Require an EOT to satisfy the outgoing ENQ link
                                 test request. Normally an incoming link test re-
                                 quest (ENQ) or a good incoming packet will satisfy
                                 the system's link test request.

simplextransmits   Because there is no acknowledgment (positive or
                                 negative) on simplex connections the simplex
                                 packet will be sent this number of times to make
                                 sure it gets through. The remote end keeps track
                                 of the last 64 (typically) serial numbers to prevent
                                 duplicate packets. This field is usually set to 1 or
                                 3.

tict	Inter-character timer. The amount of time in milliseconds to wait for additional characters once we start reading from the remote end.
tnri	No response idle timer. The amount of time in milliseconds to wait after sending a packet for the response. The TNPP specification also has a tnrb which we don't use because of the way data is transmitted (i.e. At the time we are reading from the remote our packet transmit is not busy).
tnre	No response ENQ timer. The amount of time in milliseconds to wait for the link test response.
thold	The amount of time in the future to reschedule the packet when an RS is received.
tidle	If there is no activity on this port in tidle milliseconds a link test is sent.
cretrymax	The maximum number of times a packet may be resent before it is discarded. The default is 6.
choldmax	The maximum number of times a packet may be RS'd by the remote before it is discarded. The default is 24.
cenqmax	The maximum number of link test failures before the port is marked faultoff. The default is 6.

WCTP services support the following additional fields:

wctpversion	The default and only supported version is currently WCTP-DTD-V1R1.
wctptoken	Token to send. Default is 0001.
dtdurl	The URL for the WCTP DTD. Default is http://dtd.wctp.org/wctp-dtd-v1r1.dtd.
minpoll	The minimum polling time in seconds a client is allowed. 0=disabled. This may be up to 3600 seconds.

mingetstatus	The minimum time in seconds to query the status of a message. 0=unlimited. This may be up to 3600 seconds.
contactemail	The contactemail to send for wctp-VersionQuery.
contactphone	The contactphone to send for wctp-VersionQuery.
contactwww	The contactwww to send for wctp-VersionQuery.
contactinfo	The contactinfo to send for wctp-VersionQuery.

6.2   modemtype

The modemtype table holds the definitions for various modems. The OMEGA-LX comes with definitions for US Robotics Sportster, US Robotics Courier, Multitech ZDX, UDS 2440, and UDS v.3225/v.3229.

6.2.1   Fields

modemnum	A unigue number for this modem entry.
modemname	A description for this modem.
init1	The first init string to send to the modem. This is typically the command to load factory settings.
init2	The second init string to send to the modem.
skipreset	Enable skipping the ATZ to reset the modem before sending the initialization strings.
hangupmethod	Specify the modem hangup method. 0=drop DTR, 1=send +++ ATH.
netmodem	Indicates whether or not this service is connected to the Hark INM for netmodem access. The Hark INM provides up to 4 outdial modems in a 1U rackmount box.

6.3 smpproute

SMPP routing settings. SMPP destinations are based on the subscriber id.

6.3.1 Fields

smpproutekey   A unique number used as the primary key for this
                      database record.

startid   The starting ID for this route.

endid   The ending ID for this route.

servicenum   The service number to deliver the messages to.

6.4   tnpproute

TNPP routing settings.

6.4.1 Fields

tnpproutekey
: A unique number used as the primary key for this database record.

destination
: The TNPP destination address to which the packets are to be sent.

status
: Status of this route entry. Valid values are:
  0 Off-line
  1 On-line
  2 Fault-off

servicenum
: The remote service to use for sending the TNPP packet. See the service table for more information.

remapsource
: If yes, uses NewSrc for the TNPP source ID. Otherwise it uses the existing source ID.

newsource
: Used for remapping the TNPP source packet.

remapdest
: If yes, uses New destination for the TNPP destination ID. Otherwise it uses the existing destination ID.

newdest
: Used for remapping the TNPP packet being sent.

remapinertia
: If yes, uses New inertia for the TNPP inertia. Otherwise it uses the existing inertia.

newinertia
: Specify a different inertia for the outgoing packet.

remappriority
: If yes, uses newpriority for the TNPP priority. Otherwise it uses the existing priority.

newpriority
: Specify a different priority for the outgoing packet. Both setting/clearing the priority bit in CAP packets and setting the priority level in EXTCAP packets are supported.

remaprfchan
: If yes, uses New RF channel for the TNPP RF channel. Otherwise it uses the existing RF channel.

newrfchan
: Specify a new RF Channel for the outgoing packet.

remaprfzone   If yes, uses New RF zone for the TNPP RF zone.
                                         Otherwise it uses the existing RF zone.

newrfzone   Specify a new RF Zone for the outgoing packet.

6.5 outputgroup

Output group settings. Output groups are used to group TNPP routes and paging services. It may contain tnppgroup records (which in turn point to tnpproute records) and paginggroup records (which point to service records).

6.5.1 Fields

groupnum	A unique number used as the primary key for this database record.
name	A descriptive name for this output group.
outputrate	Only supported when opage is enabled.

6.6   tnppgroup

TNPP group settings. Group tnpproute records together. A message sent to this group will be sent to all the tnpproute services in this group.

6.6.1   Fields

groupnum   A unique number used as the primary key for this
                              database record.

sequencenum   A sequence number to make this record unique.

tnpproute   The tnpproute record to send messages to.

6.7   paginggroup

Paging group settings. Group services together. A message sent to this group will be sent to all the services in this group.

6.7.1   Fields

groupnum   A unique number used as the primary key for this database record.

sequencenum   A sequence number to make this record unique.

servicenum   The service to send messages to.

6.8   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.

6.8.1   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.

allowpoll	Allow WCTP enterprise message polling. Default is no.
sequencenum	The current sequencenum for WCTP enterprise polling.
lastpoll	Timestamp for the last WCTP enterprise poll.
name	The subscriber's name. This field may be up to 64 characters.
companyname	The subscriber's company name. This field may be up to 64 characters.
companyphone	The subscriber's company phone number. This field may be up to 16 characters.
techname	The subscriber's tech contact name. This field may be up to 64 characters.
techemail	The subscriber's tech contact email address. This field may be up to 80 characters.
techphone	The subscriber's tech contact phone number. This field may be up to 16 characters.
techfax	The subscriber's tech contact fax number. This field may be up to 16 characters.
listsubscribe	Specifies whether the user is subscribed to the wctp email list.
listemail	The user's email address to send the wctp list emails to.
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.

6.9 throttle

Recipient message throttling settings. This table defines a set of throttling values. The default values are used unless a specific throttle number is specified in the subscriber record. This differs from ipfilt throttling because this is based on the recipient no matter which protocol on which the message is received. A default throttle number to use for all recipients may be specified in the common section of omega.ini. If any of the three values (morethan, intime, disablefor) are set to zero, recipient throttling for this throttle number is disabled.

6.9.1 Fields

throttlenum	A unique number used as the primary key for this database record.
morethan	If more than this number of connections to the recipient during intime seconds are received additional messages will be blocked for disablefor seconds. Set this value to 0 to disable checking.
intime	The amount of time in seconds to track the number of incoming messages for this recipient.
disablefor	The amount of time in seconds to disable connections from for the recipient.

6.10   virthost

Contains the virtual host definitions.

6.10.1   Fields

domainname | The domain name to accept messages for.

enabled | Specifies whether or not to allow connections for this domain. This allows you to temporarily disable a domain.

allowemail | Specified whether or not to accept email for this domain.

directory | The sub-directory under www to use for the web pages. More than one virthost entry may use the same directory. The default directory is 'default'.

mainhref | An alternative web site address to go to when the logo is clicked. This only affects the subscriber web page logo, not the web admin logo.

mainlogo | An alternative logo to use for this host. This only affects the subscriber web page logo, not the web admin logo.

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

subjectswitches	Enable use of subject line switches for this domain. This option is typically only enabled for domains that send the body only so the sender can control which fields to send.
ldaphosts	A list of LDAP servers with which to authenticate subscriber ID's. The names should be specified with hostname:portnum. Multiple servers are supported by separating the hostname:portnum pairs with spaces. For example, "server1.example.com:389 server2.example.com:389".
sendpageidname	The name of the pager ID field on the Send a Message web page. If this is left blank "pin" will be used.
sendpagemessagename	The name of the message text field on the Send a Message web page. If this is left blank "message" will be used.
sendpagefromname	The name of the from text field on the Send a Message web page. If this is left blank "from" will be used.
sendpagesubjectname	The name of the subject text field on the Send a Message web page. If this is left blank "subject" will be used.
maxrecipients	The maximum number of recipients to allow in a single session for this virtual host.
enabledisclaimer	Enable the disclaimer web page after submitting a message before accepting the message for delivery.
enablecaptcha	Enable graphical confirmation page before accepting the message for delivery.
appenddomain	When set, append the domainname field to the recipient address for any incoming message for this domain.

ldapbase	The base to start the search.
ldapbinddn	The Distinguished Name (DN) used for binding.
ldappassword	The password to login to the LDAP server.
ldapfilter	The search filter to use for the LDAP query.
ldapvalidattr	The name of the valid attribute. This is the attribute that is retrieved from the LDAP server to test if this is a valid subscriberid or not. If the value retrieved is either upper or lower-case Y or is a non-zero number the subscriber id is considered valid. This field may be up to 32 characters long.
ldaplcosattr	The name of the lcos attribute. This is the attribute that is retrieved from the LDAP server to specify the lcos. This field may be up to 32 characters long.
ldapserviceattr	The name of the service attribute. This is the attribute that is retrieved from the LDAP server to specify the service to use for the incoming ID. This field may be up to 32 characters long.

6.11 idblock

Idblocks allow you to define ranges of incoming numbers for delivery to a common output. Incoming Ids which belong to more than one block will be accepted by the block with the smallest range which includes the ID.

After finding a match the incoming number can be transformed by different methods. First, if StripChars is specified and they match the beginning of the incoming number those digits matching will be stripped. If StripChars is not specified and StripLen is, the number of digits in StripLen will be stripped from the beginning of the incoming number. Next if there are digits in Prefix they will be prepended to the incoming number and any digits specified in Append will be appended to the end of the incoming number. The maximum length of the resultant number must be 16 or less. If there are more Prefix digits than will fit the Prefix will be truncated to make the resulting number less than 16 digits long. After that if the Append string will cause the digits to be more than 16 the Append digits will be truncated so that the resulting digits will be less than 16.

6.11.1 Fields

blocknum	A unique identifier for this ID block.
name	A descriptive name for this ID block.
enabled	Specifies whether this ID block is enabled to accept incoming connections with an ID in this range.
startid	Starting number for this ID block.
endid	Ending number for this ID block.
outputgoup	Specifies the output group to use for message notification.

allowsource
Specifies the sources that are allowed to send messages to this block. The value for this field is computed by adding the values in the following list together:

1	GCP
2	HTTP
4	SMPP
8	SMTP
16	SNPP
32	TAP
64	TNPP
128	WCTP

prefix	Digits to prepend to the incoming ID.
stripchars	Digits to strip from the beginning of the incoming ID. The system will strip the digits only if they exactly match the digits of the beginning of the incoming ID.
striplen	If StripChars is empty and this field is set to a number greater than zero, the corresponding number of digits will be stripped from the beginning of the incoming ID.
append	Specify the digits to be appended to the end of the incoming ID.
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.

6.12   subscriber

The subscriber table allows you to setup specific overrides for the idblock table. When adding a subscriber make sure to also add pager records for the subscriber. The subscriber table specifies how a message is allowed to be received for a subscriber. It is strictly an input table, the pager table defines how messages are sent out for the subscriber.

6.12.1   Fields

subscriberid	The subscriber ID. This is typically the subscriber's 10-digit pager number without dashes or other puncuation.
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	Specifiy 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:

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.
throttlenum	Incoming message throttling group.
maxmessagelen	The maximum message length the subscriber is allowed. Other limits may lower this limit. For example, certain outputs may have shorter message limits. The output may be set to split messages if needed.
prefixtext	Up to 16 character text message that can be prefixed to the outgoing message. See also messagemodifier below for rules on when to prefix. Also see allowmsgmodifier in the pager table to specify a pager specific override.
suffixtext	Same as prefix text except that it is appended to the message if there is room in the output.
messagemodifier	Specifies when to prepend the prefixtext or append the suffix text. It is a bitfield and is described by the table below. Add the values together to support all possible combinations.

0	Do not prepend or append
1	Prepend prefixtext to primary pager
2	Prepend prefixtext to non-primary pagers
4	Append suffixtext to primary pager
8	Append suffixtext to non-primary pagers
16	Trim trailing whitespace
32	Trim leading whitespace
64	Enable message filters

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 (00:00) 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_URL and SMARTHOST_TIMEOUT are specified in the [common] section of omega.ini. Values 1 through 7 are reserved for resetting the countdown callcount on Sun through Sat respectively. The value of 9 is reserved for resetting on week of month.

6.13 aliases

The alias table allow multiple personalized names to refer to specific subscribers.

6.13.1 Fields

alias   The alias to use. The value for this field may be up to 128 characters. Do not include the domain name for email aliases. This value should be just that part to the left of the @.

subscriberid   The subscriber record to use for this alias. The subscriber must exist in the subscriber table.

6.14   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 message is stored in the database, but not actually sent anywhere. Records may be added in this table for a subscriber to specify multiple delivery devices. For example, a TNPP pager and email.

6.14.1   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.

allowmsgmodifier
: Allow the subscriber prefixtext and suffixtext to apply to this pager. Both the pager.allowmsgmodifier and the subscriber.messagemodifier must pass for the text to be prepended or appended. If the subscriber messagemodifier allows the prefix or suffix to be added and this field is set to false the outgoing message will not be modified.

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

6.15   tapprofile

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 conjuction with the tappassword table.

6.15.1   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.'.

6.16   tappassword

Allows custom TAP timeouts based on automatic mode password used.

6.16.1   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.

6.17 emailfilt

Subscriber maintainable email filters.

6.17.1 Fields

emailfiltkey	A unique key for the filter record.
subscriberid	The subscriberid this filter belongs to.
enabled	Whether or not this filter is active.
action	Set to 'A' to accept the email or 'D' to deny the email.
if	The following are the allowable values:

1	Sender
2	Subject
3	Message Body
4	Priority
5	To
6	Forward for IP

verb	The following are the allowable values:

1	Contains
2	Doesn't contain
3	Is
4	Isn't
5	Begins with
6	Ends with

pattern	The character pattern to match.
stripmatch	When enabled the matching pattern is removed from the message.

Chapter 7

Program Descriptions

The following sections describe the executables that make up the OMEGA-LX application. For Linux systems the base directory is /opt/omegalx.

7.1 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.

7.2 System programs

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

7.2.1 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.

7.2.2 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.

7.3 Protocol servers

7.3.1 gcpd

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

The GCP server supports both RS-232 and TCP/IP connections. Multiple connections can be defined for multiple serial ports and multiple sockets. The GCP server also supports multiple connections per TCP/IP listen port.

The Omega also supports a limited computer interface using GCP. Please see the "Computer Interface" section of the "Database Maintenance" chapter for more information. The following commands are supported:

- @RV read version.

- @PO page out

- @CR create record

- @RE read record

- @DR delete record

- @MR modify record

- @SN set node

- @LV login

- @QT quit (not part of Glenayre spec)

- @RK send rekey command to pager (not part of Glenayre spec)

- @CD send clear device command to pager (not part of Glenayre spec)

- @GK generate random encryption key (not part of Glenayre spec)

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.

Commands not listed above 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.

7.3.2 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. If the system is using Apache for a reverse proxy (which is the default configuration) any virtual hosts you define must be added to the /etc/httpd/conf.d/zz-omega.conf file and Apache restarted with `service httpd restart`.

WCTP and webadmin can also be configured to be handled by the HTTP server.

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

7.3.4 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.

Long messages are now supported using the SAR TLV and UDH methods also. UDH seems to be better supported by carriers and SMPP aggregators.

7.3.5   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.

If the system is using the Postfix mail server in front of the Omega-LX smtpd server virtual hosts will also need to be added to the Postfix configuration in addition to the omegalx database. Please see the "Email - Postfix" section in the "Configuration" chapter for more information.

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.

Subject line switches

If the protocol option PROTOPTION_SMTPSUBJSWITCHES is enabled certain subject line switches are supported. Also, the subjectswitches field in the virthost

table must be enabled for the domains you wish to allow senders to control the output fields. Typically subject line switches are only enabled on "send body only" virtual hosts to give the greatest control to the sender. Subject line switches add to the sendfields for the virthost. These define which fields of the incoming email message will be delivered. Switches must adhere to the following rules:

- Switches may be used with any email domain name supported in the system's virthost table.

- Switches must be located on the Subject line.

- Switches may be in any order. (e.g. -a Test, Test -a Subject, Test Subject -a, or Test -s Subject -a, etc).

- Switches may be mixed with the Subject line text. (e.g. Test -a -s Subject).

- Switches may be combined. (e.g. Test -as Subject).

- There must be white-space (space or tab) before and after a switch. White-space is not needed after the switch if it is the last item on the subject line.

- Switches are case-sensitive. The switch must be lower-case. (e.g -a not -A).

Switch	Name	Description
-a	Author	Include the "real name" from the email "From:" field
-d	MDN	Send the message disposition notification field
-e	Emailfrom	Include the email address from the email "From:" field
-s	Subject	Include the email "Subject:" field
-m	Message	Include the message body of the email
-c	Count	Include a word count
-t	Timestamp	Include a time stamp

7.3.6 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>

The following level 3 commands are supported when PROTOPTION_SNPPLEVEL3 is enabled:

- 2WAY

- NOQUeueing

- ACKRead <0—1>

- MSTA

- KTAG

- RTYP

- MCRE

7.3.7 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)

7.3.8 thinclient

Processes the thin client output queue and sends any messages received to the recipient or the original sender if a recipient is not specified. This application uses the thinclient database which is created separately from the main Omega-LX database.

7.3.9 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.

7.3.10 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

7.4 Maintenance programs

7.4.1 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><DEL>. If for some reason the screen gets out of sync, pressing <CTRL><R> will redraw the screen.

7.4.2 monitor

Monitor system for programs and deliver alarms if needed. Monitor performs the following functions:

- Monitor available memory and send alarms if necessary

- Monitor available hard drive space and send alarms if necessary

- Send periodic test pages

- Scan message database for future delivery messages and send them

- Scan message database for expired messages and remove them

The monitor program will check the available disk space, free memory and future delivery requests every SCAN_TIME seconds.

7.4.3   sptest

The sptest program is for sending alarms via the syspage server. By default the
sptest program will send a test alarm at error level 255. Or it can be used to send a
specific message to the alarm server by passing in an argument. For example:

```
sptest "This is my custom test alarm message"
```

7.4.4   pst

The pst script displays a process list of just the Omega-LX programs. In addition to
the process ID, the number of threads and memory usage are also displayed for each
program.

Chapter 8

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.

The configuration for billing logs is in the service table in the database. The logtype must be set to log billing records. You may log incoming messages, outgoing messages, or both for each service. Enable logheader to write a field header at the beginning of each day's billing log. The logfile format can be set to CSV for importing into a spreadsheet or database, or TAB delimited. Finally, the logfields contains a comma-separated list of the field names in the order specified to write to the billing log.

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/opt/omegalx/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/opt/omegalx/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
```

Network traffic can also be monitored with the iftop command. This is not included with the base system, but can easily be installed with the following:

```
wget http://download.fedora.redhat.com/pub/epel/5/x86_64/epel-release-5-4.noarch.rpm
rpm -ivh epel-release-5-4.noarch.rpm
yum install iftop
```

If you are running an i386 system replace the x86_64 in the above with i386.

9.1.3   Postfix

With all the SPAM on the Internet it is possible that some bad messages will be stuck in the Postfix mail queue for a while before they are purged. This is not normally a problem, but if you have an abnormally large mail queue that is not getting smaller you can manually clear the deferred messages.

To view the current Postfix mail queue type `mailq`. To remove all the deferred messages (that are usually due to a bad DNS name) type the following: `postsuper -d ALL deferred`.

9.1.4   DRBD

To fix a DRBD "split brain".

on bad node:

```
drbdadm secondary all
drbdadm disconnect all
cat /proc/drbd  (should now show ''Secondary/Unknown'')
drbdadm invalidate all
drbdadm connect all
```

on good node:

```
drbdadm connect all
```

`cat /proc/drbd` should now show Primary/Secondary and UpToDate on the primary machine.

9.1.5 RAID

Make sure both drives in the mirror are bootable.

```
grub
root (hd0, 0)
setup (hd0)
root (hd1, 0)
setup (hd1)
quit
```

To replace a failed drive display the current RAID status with `cat /proc/mdstat`. If you see U␣ instead of UU for each filesystem the RAID is in a degraded state. First determine which drive has failed. It may be /dev/sda or /dev/sdb. In the following example we will assume it is /dev/sdb.

If there is no F after the failed filesystem perform the following steps replacing the /dev/md and the /dev/sd with the proper values:

```
mdadm --manage /dev/md0 --fail /dev/sdb1
mdadm --manage /dev/md1 --fail /dev/sdb2
mdadm --manage /dev/md2 --fail /dev/sdb6
mdadm --manage /dev/md3 --fail /dev/sdb5
mdadm --manage /dev/md4 --fail /dev/sdb7
mdadm --manage /dev/md5 --fail /dev/sdb3
mdadm --manage /dev/md6 --fail /dev/sdb8
```

Now the drive should show as failed. Remove the failed drive from the array by typing the following:

```
mdadm --manage /dev/md0 --remove /dev/sdb1
mdadm --manage /dev/md1 --remove /dev/sdb2
mdadm --manage /dev/md2 --remove /dev/sdb6
mdadm --manage /dev/md3 --remove /dev/sdb5
mdadm --manage /dev/md4 --remove /dev/sdb7
mdadm --manage /dev/md5 --remove /dev/sdb3
mdadm --manage /dev/md6 --remove /dev/sdb8
```

If we replace the drive right now, the OS would assign it a new device, so instead replace the drive and reboot with `init 6`.

After rebooting the new drive should come up as /dev/sdb. The new drive must be partitioned to match the existing drive.

```
sfdisk -d /dev/sda | sfdisk /dev/sdb
fdisk -l
```

Now the filesystems on the new drive can be added to the mirror.

```
mdadm --manage /dev/md0 --add /dev/sdb1
mdadm --manage /dev/md1 --add /dev/sdb2
mdadm --manage /dev/md2 --add /dev/sdb6
mdadm --manage /dev/md3 --add /dev/sdb5
mdadm --manage /dev/md4 --add /dev/sdb7
mdadm --manage /dev/md5 --add /dev/sdb3
mdadm --manage /dev/md6 --add /dev/sdb8
```

9.1.6 Database

Get a list of databases:

```
select datname from pg_database;
```

Get a list of tables in current database:

```
select tablename from pg_tables where tablename not like 'pg_%' \
  and tablename not like 'sql_%';
```

Get a list of field names and attributes for a table:

```
\d tablename
```

Get a list of indexes for a table (replace tablename with the tablename):

```
SELECT relname FROM pg_class WHERE oid IN
  (SELECT indexrelid FROM pg_index, pg_class
   WHERE pg_class.relname = 'tablename' AND
         pg_class.oid = pg_index.indrelid AND
         indisunique != 't' AND
         indisprimary != 't')
ORDER BY relname;
```

Get a list of tables with foreign keys referencing a particular table (replace tablename with the tablename):

```
select t.constraint_name, t.table_name, t.constraint_type,
       c.table_name, c.column_name
from information_schema.table_constraints t,
     information_schema.constraint_column_usage c
where t.constraint_name = c.constraint_name and
      t.constraint_type = 'FOREIGN KEY' and
      c.table_name = 'tablename';
```

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/opt/omegalx/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

Maintenance

To keep your system running at peak performance there may be certain maintenance procedures which should be routinely performed.

10.1   Backups

10.1.1   Database

Backup the database:

```
pg_dump -U postgres omegalx -f backup.sql
```

Restore the database:

```
psql -U postgres -d omegalx -f backup.sql
```

10.1.2   Operating system

To backup the Linux configuration files, place a floppy in the floppy drive and type the following:

```
tar czvf /dev/fd0 --files-from /root/backup_files
```

The application directory may also be backed up using a writable CD. First make sure that the directory will fit on a CD by typing the following:

```
du -sk /opt/omegalx
```

Once the `du -sk` returns less than approx 650000 (or 700000 for 80 minute CDs), you can copy the entire /opt/omegalx directory to CD with the following command:

```
mkisofs -R /opt/omegalx | cdrecord -v fs=6m speed=32 dev=ATA:1,0,0 -
```

The 1,0,0 may be different on your system. Type the following to see what the three numbers are for the CD burner in your system:

```
cdrecord -scanbus dev=ATA
```

10.2   Daily maintenance

None at this time

10.3   Weekly maintenance

10.3.1   Software and Security Updates

There will not necessarily be software or security updates each week, but you may wish to check for them each week. See the "Operating System Updates" section for more information on the update procedure.

10.4   Monthly maintenance

10.4.1   Filters

Depending on the installation site, the filter in the front of the Omega may need to be vacuumed. Use the following procedure if you need to remove the filter to clean it:

- Open the front of the Omega chassis by turning the key knob to the horizontal position (you may need to use the key).

- Using a #2 phillips screwdriver remove the two screws on each side of the front cover which hold the cross-hatched plastic filter retainer in place.

- Remove the cross-hatched plastic filter retainer and filter.

- Clean the filter.

- Reinstall filter by reversing the steps used to remove it.

Chapter 11

High Availability

11.1   Load Balancing

By default the OMEGA-LX supports load-balancing. This allows multiple servers to accept incoming connections and deliver them to the pagers or other messaging devices. To support load balancing a separate database server is now required. For redundancy the separate database server can be setup in a clustered configuration.

Load balancing is different from clustering because the servers do not need to be identically configured. Also, load balancing can more easily be added after installation. Clustering requires a specific filesystem to be created and must exactly match size and configuration on the two machines. Load balancing supports filesystems of different sizes and even different types and supports more than two machines. Another advantage with load balancing is there is no down time while the cluster configuration fails-over from the primary to the secondary machine. With load balancing all the machines are accepting connections all the time. The disadvantage of load balancing is with serial connections. Because all of the machines are active at the same time, multiple serial ports are needed to connect to paging terminals. For example, there are two OMEGA-LX servers in a load balanced configuration and each need to send TNPP over RS-232 to a paging terminal. The paging terminal will need an incoming TNPP serial port configured for each of the OMEGA-LX servers (in this case two serial ports).

Another factor to consider with load balancing is that external load balancers are required which can significantly increase the cost of the system. Hark does not supply load balancers or recommend any particular product.

Chapter 12

Change summary

12.1   Changes in 6.2

- NMS CG6x6x telephony board support has been updated to version 9.0.8 using the 64-bit drivers. It is no longer necessary to install the 32-bit version of omegalx in the 64-bit CentOS.

- Telephony board configuration has been moved from the ini file to the database.

12.2   Changes in 6.1

-

12.3   Changes in 6.0

-

12.4   Changes in 5.3

-

12.5   Changes in 5.2

- FreeTDM support for using Digium T1 boards for numeric paging.

- SMPP support client-side bind transceiver

- SMPP support multiple incoming short codes for mobile originated email to specify the domain name of the sender

12.6   Changes in 5.1

If you are installing telephony support you will need to wget the i686 version of Omega-LX `wget http://support.harktech.com/dl/rhel5-i386/omegalx-5.1-1.rhel5.i686.rpm` and install it manually with `rpm -ivh omegalx-5.1-1.rhel5.i686.rpm`. Also you will need to install the i386 version of the postgresql libraries with `yum install postgresql84-libs.i386`. Even though you are installing on an x86_64 host, the i686 version is required for using the Dialogic CG drivers. If you are not using the nmsd program you can just install the x86_64 version using the yum update above.

- support Dialogic CG-6x6x boards for numeric paging over T1 interfaces

- send configurable message to numeric/alpha pager when their countdown limit is exceeded

- can now configure a web user to show password fields in the web admin

- system now automatically gets message status rather than wait for client poll

- traffic stats now stored for doing traffic queries between time periods

- TNPP dial out now supports batch count and batch timer

- handset replies to email now quotes original email

- send HTTP and WCTP now supports SSL

- add sendfields support to idblock

12.7   Changes in 5.0

- add a BILLING_HEADER to prefix the billing logs for easier import into Excel/Access

- improvements to SMPP server to act as an SMSC (previously we only supported acting as an ESME)

- add covrgn table for incoming TNPP cap paging subscriber lookup

- merge syspage support into omegalx (from standalone program)

- support ANI in subaccess and virthost sourceaddress fields also

- add Thin Client Server support

- now uses GNU gettext for internationalization and localization support - currently only supported languages are en_US and fr_CA

- add support to only send one email when a subscriber has been temporarily shutoff due to countdown limit (countdown notify)

- add ipfilt and throttle notify email addresses to alert NOC that a subscriber has been throttled

- fix rtview display after a recent OS update

- support sending real-time response from SMPP submit_sm back to client connection

- support for load balancing TNPP output like we already had for SMPP

- support sending SMPP destination_port and source_port TLV - beginning of alternate port SMS support

- support limiting subscribers to a maximum output rate - for example don't allow a subscriber to send more than one message per minute out a TNPP port

- copy message data to up to 7 additional geo-redundant servers

- support sending billing logs to a separate SQL database

- support maximum simultaneous network connections per client IP address

- support maximum connection time to prevent clients from keeping a connection open indefinitely

- support stripping confidentiality notices (or other fixed text) from messages

- 2-way SNPP

12.8 Changes in 4.5

- TNPP can now route additional protocols based on TNPP node ID

- web paging captcha and disclaimer updates

- LDAP updates

- add a network connect timeout (default OS timeout is way too long)

- fully supprt QP and B64 in email From and Subject headers

- support finding subscriber by TNPP capcode also

- config support forcing subscriber max message len in case we prefix with email fields

- fix problem with max choices in WCTP multichoice support

12.9   Changes in 4.4

- TAP and modem improvements

- add anti-spam settings to virthost table

- more French language improvements on web pages (buttons)

12.10   Changes in 4.3

- send_gcp performance fixes

- support iso-8859-1 in subject

- create poolthreads for further opage throughput

- add pager replyto support for outgoing SMTP

- HTTP sendpage convert UTF-8 accented character to English equivalent

- opage throughput improvements

12.11   Changes in 4.2

- added n4,n5,n6 to tapprofile

- additional range checking for tnpp cap fields

- support prefixtext and suffixtext

- GCP support fields 00 and 000 to read all fields

- fix LDAP lookup support - broken in recent OS update

- SMPP now supports output load balancing

- fix captcha support after recent web page changes

- disable autocomplete on web page password fields for PCI compliance

- add Glenayre style egroup to subscriber table

- support compressing billing logs

- configurable logtype per service

- WCTP now support data ipfilt

- new license key format

12.12 Changes in 4.1

- add rest of GCP fields for 6.1 and 8.0

- support tnppidblock to translate incoming TNPP pager numbers from 8 digit to 10 digit

- move WCTP contact/version info from config to database

- SMTP throttle code return value now configurable

- add protocoloption to service so different snpp/wctp ports can requirelogin and not require login

- move SMTP/SNPP hello message from config to database so different ports can answer differently

- add virtual port support TNPP link test

- add TNPP virtual port support for Glenayre TNPP over UDP

- liboxgen/check_id don't check if msgfrom exists for messageid lookup

- support Glenayre data page length fields in gcp

12.13 Changes from IMG-LX to OMEGA-LX 4.0

- leave room in TNPP queue if packet needs to be re-inserted due to RS

- update random number generation

- support Microsoft non-standard MDN Return-Receipt-To

- support Message-Disposition-Notification

- support output groups

- httpd support multiple languages (English and French for now)

- add throttle/throttlesession support

- support automatically upgrading database schema after update

- change input/output rates from packets per second to packets per minute

- supports TNPP CAP paging

- supports multiple pagers per subscriber record

- supports outputgroups which work like Glenayre coverage regions

- supports active-passive server clustering in addition to the load-balancing support in the IMG-LX

- additional columns in virthost table for branding

- ability to set SMPP source address based on SNPP/WCTP login

- lcos table to define incoming limits

- smtp, snpp, and wctp can now listen on multiple ports. This, for example, allows a wctp port to be setup requiring login and a separate port that doesn't require a login.

- opage created for outgoing paging

- beginning of support for SIP-based voice mail

- idblock can now also limit source access (CHECK_SOURCE)

- moved LDAP configuration from global ini to virthost

- support Hark INM network attached modems for TAP outdial

- subscriber web maintenance support

- email now supports parsing text/html if no text/plain part

- supports running with dropped privileges

- supports automatically updating the database schema if needed

- support routing incoming TNPP packet to TAP outdial modem based on TNPP destination node address

Chapter 13

Warranty Information

<u>WARRANTIES</u>

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. If this product is licensed as a "Software Only" product, the warranty shall be limited to one year.

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.

<u>DISCLAIMER OF WARRANTIES</u>

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.

<u>BREACH OF AGREEMENT</u>

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.

<u>ALTERATIONS AND CHANGES</u>

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 14

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