Omega TNPP Router
Version 3.15

Hark Technologies

October 11, 2007

Copyright

Copyright © 2005 Onix Electronic Systems, LLC. All rights reserved. No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, photocopying, recording, or otherwise, without the prior written consent of Onix Electronic Systems, LLC. 8105 Bankshire Trl, North Charleston, SC 29420

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, LLC. assumes no liability resulting from errors or omissions in this document or the use of the information contained herein.
Onix Electronic Systems, LLC. 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, LLC., 8105 Bankshire Trl, North Charleston, SC 29420.

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

With the merging of paging companies, sharing of channels, and formation of roaming agreements for paging customers, TNPP, or Telocator Network Paging Protocol, has grown to become the standard protocol used to route paging traffic and data between multiple paging service providers.

Each of the service providers are linked or connected to other service providers via TNPP networks. These networks allow the source or originator to transmit paging data to a particular destination. The paging calls can then be routed over large geographic areas; for example, statewide, regional, or nationwide.

The paging data is sent in packets, with each packet containing one or more page blocks. The page blocks contain information about the page, the destination of the page, and the source of the page. Each page block may be identified as a Capcode or ID page. Since the destination address is contained within each packet being distributed, the node that is receiving the packet will know how and where to re-transmit the packet. The redistribution of the packets is performed according to the receiving nodeś internal routing tables.

The Omega TNPP Router serves as a central node, or hub, on a TNPP network, facilitating the exchange of traffic between the independent paging terminals located in various locations.

The Omega serves as an intermediate node on the network. Each port on the Omega has a TNPP ID, but this is only used for sending the initialization packet. Each port may share an ID or have a unique ID for those situations that require it. The TNPP packets enter the router from any source location and are routed to other locations based on the internal routing tables. The packets may be accepted or blocked, and even modified, based on the filter table.

1.3 Features and Benefits

- Supports both RS-232 and Network TNPP ports
- Real-time monitoring of port statistics
- Incoming packets may be routed to one or more output ports
- Dedicated RS-232 or Modem dialup connections are supported
- Incoming packets may be blocked by combinations of capcode, source, block type, destination and page type
- Support serial data rates up to 115,200 baud
- Each port can be configured for full-duplex, simplex input, or simplex output
- Translation of source address, destination address, inertia, channel and zone
- System alarm program to send alarms in various error conditions
- Configurable billing logs
- Extended cap packets and Flex pages are supported

- Remote control using an encrypted secure shell
- Optional clustering software to maintain high availability

1.4 Support Services

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

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

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

For technical support between the hours of 7:30 AM and 4:30 PM Eastern Time, Monday through Friday, excluding holidays, call 843-767-1775. For technical support outside of normal business hours or on holidays, call 843-767-1775. The voice mail operator will answer your call. This number allows you to leave a message for normal business matters, or initiate a page for immediate technical support. The voice mail attendant will lead you through the appropriate procedures. For matters that do not require an urgent response, leave a voice mail message within the general mailbox.

For urgent matters that require that you speak to an on-call technician, select the appropriate key identifying the product for which you need technical support. After the technician's greeting, leave a short message with the area code and phone number at which you can be reached. The on-call technician will be paged and will return your call.

Phone:	843-767-1775
Fax:	518-448-6698
Web:	http://harktech.com
Sales email:	sales@harktech.com
Support email:	support@harktech.com

Chapter 2

Installation

2.1 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 null modem serial cable between the serial ports on the back of the two computers. Also 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. See the "Cluster" chapter for more information.

2.2 Operating System

The Omega TNPP router is available as a turnkey system or as a software only application. Both use the Linux Operating System. Turnkey systems already have the operating system and application installed and setup. 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.

2.2.1 Software only - Installing the OS

Centos Linux 4.2 or greater is used for the Linux-based Omegas. This can be downloaded from http://www.centos.org . Software only Linux-based Omegas will include the Centos install CD so it is not necessary to obtain it on your own.

Make sure that you have a keyboard, mouse and monitor plugged into your server. Also an ethernet cable would be a good idea, but not necessary at this point. 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 CD.
- Boot the computer. You will see a Centos 4 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.
- You should now see the disk partitioning screen. Select the “Manually partition with Disk Druid” radio button and 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.
- You should now be in Disk Druid. Click New to create a new partition.

- You should now see the “Add partition” window.
- Set the mount point to /boot. Check the “Force to be a primary partition” checkbox. Click OK.
- Click New to add another partition.
- Set the mount point to /. Set the size to 5000. Check the “Force to be a primary partition” checkbox. Click OK.
- Click New to add another partition.
- Set the filesystem type to swap. Set the size to 2048. Check the “Force to be a primary partition” checkbox. Click OK.
- Click New to add another partition.
- Set the mount point to /var. Set the size to 10000. Click OK.
- Click New to add another partition.
- Set the mount point to /opt. Set the size to 10000. Click OK.
- Click New to add another partition.
- Set the mount point to /var/opt. Check the “Fill to maximum allowable size” checkbox. Click OK.
- Click Next
- You should now see a screen with “The GRUB boot loader will be installed on /dev/sda”. You don’t need to change anything here. Just click Next.
- Now you will see the Network Devices setup.
- If you are using DHCP click next, otherwise click Edit and change the IP settings. Make sure “Activate on boot” is checked. If you are unsure at this point, leave it set to DHCP. This can always be changed later. Hostname should be set manually. Pick a unique hostname in your domain. For example, tnpplx.yourdomainname.com.
- Click Next
- Leave “Enable Firewall” checked. Check “ssh” to allow encrypted shell access from remote locations. Change “Enable SELinux” to Disabled.
- Click Next
- “Select the default language for the system” and click Next.
- Select the appropriate timezone and click Next.

- Enter a password for the root user. You will need to enter it twice. The password will not show on the screen. Make a note of this password. You will need it to login later. Click Next to continue.
- Check the "Customize software packages to install radio button" and click Next.
- Scroll to the bottom and check "Minimal" to install the minimal set of packages and click Next.
- Click Next again.
- Next you should see a few popup windows stating that the system is formatting the various filesystems previously setup. Then the system will transfer the install image to the hard drive and prepare RPM transaction.
- Next you should see a progress bar with package names listed below it. The names will probably go by fairly quickly. This step only takes a few minutes on a relatively fast computer (2.4GHz Pentium 4).
- Next you will see "Performing post install configuration" and "Installing boot loader".
- When you see "Congratulations, the installation is complete" the CD will automatically eject. Remove the CD from the drive and close the CD drive.
- Click Reboot to reboot the computer.

Now that the system has been installed and rebooted you will see a lot of text messages display on the screen. Most of them won't mean anything to you. Ignore any errors about the "Intel Microcode Update". Not all Intel processors have a microcode update to install.

At the login prompt login as **root** using the password you entered earlier.

Now we are going to install the Operating System updates and application software.

- Insert CD #2 into the CD-ROM drive.
- Type `mount /dev/cdrom` to mount the CD.
- Type `rpm -Fvh /media/cdrecorder/RPM/*.rpm`. If you have a CD-ROM drive instead of a CD-RW, replace cdrecorder with cdrom.
- To install the hardware key drivers type `rpm -ivh /media/cdrecorder/Hasp/*.rpm`.
- Type `/media/cdrecorder/clean`. This will stop and remove some unused servers.
- Type `eject cdrom` to eject the CD.

- Type `mkdir -p /opt/tnpplx/{bin,docs,logs,sbin}`
- Type `mkdir -p /var/opt/tnpplx/{debug,errors}`
- Type `init 6` to reboot the computer and run from the updated kernel.

2.2.2 Date and time

The date and time are automatically set using NTP over the Internet. The configuration file is in /etc/ntp.conf. The default settings are usually correct for most installations. The timezone will still need to be set by creating a symbolic link from the proper timezone file in /usr/share/zoneinfo to /etc/localtime. By default the system is set to US/Eastern. First remove the existing /etc/localtime by typing:

```
rm /etc/localtime
```

Next, create the symbolic link using:

```
ln -s /usr/share/zoneinfo/US/Central /etc/localtime
```

Replace US/Central with the proper timezone file. Some areas of Indiana have special timezone setting which can be found in /usr/share/zoneinfo/America/Indiana. You can view the list of timezones with the following two commands:

```
ls /usr/share/zoneinfo/US
ls /usr/share/zoneinfo/America
```

Select the name which best describes your timezone.

2.2.3 Network settings

The hostname is set in the /etc/sysconfig/network file.

The ethernet configuration is stored in the /etc/sysconfig/network-scripts directory. There are two files of interest. ifcfg-eth0 contains the configuration information for eth0 which is the ethernet connection to the network. When looking at the rear of the TNPP-LX it is the ethernet jack on the left. By default eth0 is set for DHCP. The following is an example:

```
DEVICE=eth0
BOOTPROTO=dhcp
HWADDR=00:11:09:7C:01:00
ONBOOT=yes
TYPE=Ethernet
```

You may configure your DHCP server to serve a static IP by adding the TNPP-LX MAC address (see HWADDR in the above example) to your DHCP server or you can enter the static IP information in the ifcfg-eth0 file. If the HWADDR line does not appear in your ifcfg-eth0 file the ifconfig command will display the MAC address. Type the following from the command line:

```
ifconfig eth0
```

Look for the number after Hwaddr. It will be 6 sets of two-digit hexadecimal numbers separated by colons.

The following is an example of the output from ifconfig:

```
eth0      Link encap:Ethernet  HWaddr 00:50:04:A4:D3:DE
          inet addr:10.100.1.253  Bcast:10.100.1.255  Mask:255.255.255.0
          inet6 addr: fe80::250:4ff:fea4:d3de/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:1844747 errors:0 dropped:0 overruns:6 frame:0
          TX packets:2286165 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:599961968 (572.1 MiB)  TX bytes:1963187728 (1.8 GiB)
          Interrupt:18 Base address:0x2000
```

The following is an ifcfg-eth0 file setup for a static IP address:

```
DEVICE=eth0
BOOTPROTO=static
HWADDR=00:11:09:7C:01:00
IPADDR=10.100.1.253
NETMASK=255.255.255.0
NETWORK=10.100.1.0
BROADCAST=10.100.1.255
ONBOOT=yes
TYPE=Ethernet
```

ifcfg-eth1 contains the configuration information for eth1 which is the dedicated network to the other server in a clustered system. See the "Cluster" chapter for more information on the TNPP-LX clustered system. When making changes to either of these files, type the following to have the changes take effect:

```
service network restart
```

2.2.4 Operating System Updates

From time-to-time operating system updates may become available to address security or other issues. Based on the severity and in-house testing we may request that they are installed on your system. The command to check for updates and optionally install them is:

```
yum update
```

2.2.5 Firewall and Port Security

The Omega TNPP router has a built in firewall to protect against unauthorized access and to allow restriction of access to the TNPP over TCP/IP connections. The firewall is iptables, sometimes called netfilter. There are certain entries in the firewall configuration that are needed for proper operation and remote access. By default the firewall allows connections to port 22 for ssh remote access. The firewall configuration file is /etc/sysconfig/iptables. To create a current copy of this file type the following command:

```
service iptables save
```

This should be done every time you wish to add or change the configuration file in any way. Now that you have saved the current running config edit the /etc/sysconfig/iptables. When finished making your changes as described below, you will need to restart the firewall to have the changes take affect. To load the new configuration file and restart the firewall type the following:

```
service iptables restart
```

The following is an example of the base configuration of the firewall:

```
:INPUT ACCEPT [0:0]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [13653:1014419]
:fw - [0:0]
-A INPUT -j fw
-A FORWARD -j fw
-A fw -i lo -j ACCEPT
-A fw -i eth1 -j ACCEPT
-A fw -p icmp -m icmp --icmp-type any -j ACCEPT
-A fw -p ipv6-crypt -j ACCEPT
-A fw -p ipv6-auth -j ACCEPT
-A fw -d 224.0.0.251 -p udp -m udp --dport 5353 -j ACCEPT
-A fw -p udp -m udp --dport 694 -j ACCEPT
-A fw -m state --state RELATED,ESTABLISHED -j ACCEPT
```

```
-A fw -p tcp -m state --state NEW -m tcp --dport 22 -j ACCEPT
-A fw -p tcp -m state --state NEW -m tcp --dport 8080 -j ACCEPT
-A fw -j REJECT --reject-with icmp-host-prohibited
COMMIT
```

This example has the required base entries, plus two additional entries. The two additional entries are the lines with –dport 22 and –dport 8080 in them. The –dport 22 line allows remote access to the ssh server in the Omega TNPP router. This allows one to connect to the TNPP router remotely over the internet using an encrypted secure shell as if they were on the console. A windows client is available at: http://www.chiark.greenend.org.uk/ sgtatham/putty/ . The –dport 8080 line allows remote access to the web admin page. This can be further restricted by adding a -s {ipaddr} to the line as in the below example. To restrict access to TCP port 10100 to only allow connections from IP address 1.2.3.4 add the following before the -j REJECT line:

```
-A fw -s 1.2.3.4 -p tcp -m state --state NEW -m tcp --dport 10100 -j ACCEPT
```

So now the configuration file will look like:

```
:INPUT ACCEPT [0:0]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [13653:1014419]
:fw - [0:0]
-A INPUT -j fw
-A FORWARD -j fw
-A fw -i lo -j ACCEPT
-A fw -i eth1 -j ACCEPT
-A fw -p icmp -m icmp --icmp-type any -j ACCEPT
-A fw -p ipv6-crypt -j ACCEPT
-A fw -p ipv6-auth -j ACCEPT
-A fw -d 224.0.0.251 -p udp -m udp --dport 5353 -j ACCEPT
-A fw -p udp -m udp --dport 694 -j ACCEPT
-A fw -m state --state RELATED,ESTABLISHED -j ACCEPT
-A fw -p tcp -m state --state NEW -m tcp --dport 22 -j ACCEPT
-A fw -p tcp -m state --state NEW -m tcp --dport 8080 -j ACCEPT
-A fw -s 1.2.3.4 -p tcp -m state --state NEW -m tcp --dport 10100 -j ACCEPT
-A fw -j REJECT --reject-with icmp-host-prohibited
COMMIT
```

2.2.6 System security and auditing

The Linux system chosen has proven to be secure against typical attacks. First, only essential system services are enabled. Also, the included built-in firewall is

configured to only allow in certain traffic. The sshd daemon provides a secure shell for remote access. Unlike telnet, the username and password are encrypted before being sent. Ssh can also be used to copy files using the companion utility scp. Scp also uses encrypted username and password unlike ftp. To see a list of ports currently listening on the Omega TNPP router, type the following:

```
netstat -ln
```

You should see something similiar to the following:

Proto	Recv-Q	Send-Q	Local Address	Foreign Address	State
tcp	0	0	127.0.0.1:1250	0.0.0.0:*	LISTEN
tcp	0	0	:::22	:::*	LISTEN

The Local Address shows the IP address and the port the system is listening on. For example, if you see 127.0.0.1, the system is listening on the local interface only and will not be able to receive any connections from outside computers. If you see :: or 0.0.0.0, the system is listening on all interfaces. This includes the local interface (lo0), and all of the ethernet ports (eth0 and eth1). The port number the system is listening on comes after the :.

In the above example the Local Address of 127.0.0.1:1250 shows that the syspage program is listening on the loopback interface on port 1250. This is so thatonly the TNPP router may send packets to the syspage program. The :::22 shows the sshd program is listening on all interfaces.

2.3 Application

The Omega TNPP router consists of a few applications working together to route packets and maintain the TNPP router configuration.

2.3.1 tnpp.ini

All TNPP configuration settings are stored in tnpp.ini. During our scaling testing we decided to go with an in-memory database with the settings stored in an easy-to-edit ini file. The in-memory database allows for very fast routing lookups and the ini file allows for easier maintenance using a variety of methods.

There are multiple sections in the tnpp.ini file. First is the [settings] section. This stores settings that are common to multiple programs. Next is [syspage]. This section stores settings specific to the syspage program. There is a [route] section with all of the TNPP routing information and an [alarm] section for sending alarms. Finally there are the [port] sections. These are individually numbered with a logical

port number. For example, [port1] is the first logical port. The port sections do not need to be in order.

For more information on the settings for each section see the “tnpp.ini” chapter.

Chapter 3

Clustering

3.1 Background

The Omega TNPP router can be configured to support clustering. This 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 the serial ports can not be directly connected to the TNPP router. For this reason Comtrol DeviceMaster RTS 1U rack-mount serial servers are used. These devices are connected using a 10/100baseT connection to an ethernet switch. The TNPP router then connects to the serial server and access the com ports as if they are on the TNPP router 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. In order to minimize any single points of failure, there are actually two heartbeats running. One is over a serial cable connecting the serial ports on the back of the two TNPP-LX servers. The second is over the dedicated private ethernet running on eth1.

3.2 Hardware configuration

The clustering system uses two identical computers with dual gigabit ethernet network ports. Ethernet port 0 (eth0) is setup to connect to your network. By default it uses DHCP however this can be changed by following the instructions in the "Network settings" section. Ethernet port 1 (eth1) is used for the network disk mirroring

and for a backup heartbeat. The primary heartbeat is through the serial port on the back of each computer in the cluster. These two serial ports are connected with the supplied null modem cable.

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

3.3 Setup

This section describes the clustering setup files. Most of these are already set prior to shipping, but some customization may be required for customer specific installations.

3.3.1 Heartbeat configuration

Heartbeat is the system service responsible for detecting when there is a failure and switching the services to the standby server. The heartbeat configuration is in the /etc/ha.d directory. In this directory, the ha.cf file is the main hreatbeat configuration file. The following is an example:

```
logfacility local0
baud 19200
serial /dev/ttyS0
bcast eth1
auto_failback on
node tnpplx1.harktech.com
node tnpplx2.harktech.com
ping 10.100.1.253
respawn hacluster /usr/lib/heartbeat/ipfail
```

The important options above are the serial port and baud rate. The serial port on the back of the TNPP router is /dev/ttyS0. The baud rate must match on both servers. The bcast eth1 means that the heartbeat will also be broadcast on eth1 in case the serial cable is unplugged or there is some other failure. The auto_failback feature will automatically move the services back to the primary server once the heartbeat detects that it is operational again. There are two node listings, one for each server. They must contain the Fully-Qualified Internet Host Name. Ping is used to ping a known server or router and will be used to determine if the server still has network connectivity. Multiple IP addresses may be specified to minimize false positives in case the remote server is unavailable due to maintenance or some other reason. This IP address should not be the IP address of the other server in the cluster. The respawn line is required in order to ping the remote and detect network failures.

The next important configuration file is haresources. This specifies the primary server and the resources to stop/start on fail-over. The following is an example:

```
tnpplx1.harktech.com 10.100.1.252/24/eth0 drbddisk::r0 \
Filesystem::/dev/drbd0::/opt/tnpplx::ext3 onixd
```

The first part is the fully-qualified host name of the primary server. Next is the IP address resource we are going to use externally. This will be the IP address that the remote connects to. It may be an internal IP address if you are NATing an external IP address to it. This IP address will be moved to the active server in a fail-over condition. It is not the main IP address bound to the ethernet adapter of either server in the cluster. Next drbddisk::r0 specifies that the drbddisk resource 0 is a required component. See the "Drbd configuration" section for more information on drbd. This is followed by Filesystem::/dev/drbd0::/opt/tnpplx::ext3. Filesystem indicates that heartbeat is to move the filesystem between servers in a fail-over condition. The :: separate the arguments for the component. /dev/drbd0 is the network block device which is mounted at /opt/tnpplx which is the main directory for the Omega TNPP router using the ext3 file system type. Finally we have which is the main service for the TNPP router which handles starting the syspage, httpd and tnppd processes and automatically restarting them if they should fail.

3.3.2 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. The network block device configuration is in /etc/drbd.conf. The following is an example configuration file:

```
resource r0 {
  protocol C;
  incon-degr-cmd "echo '!DRBD! pri on incon-degr' | wall ; \
sleep 60 ; halt -f";

  startup {
    wfc-timeout         5;  ## 0=Infinite
    degr-wfc-timeout  120;  ## 2 minutes.
  }

  disk {
    on-io-error detach;
  }

  net {
    # timeout           60;
```

```
    # connect-int       10;
    # ping-int          10;
    # max-buffers     2048;
    # max-epoch-size  2048;
  }

  syncer {
    rate   4M;
    group   1; # sync concurrently with r0
  }

  on tnpplx1.harktech.com {
    device      /dev/drbd0;
    disk        /dev/sda6;
    address     10.0.0.1:7789;
    meta-disk   internal;
  }

  on tnpplx2.harktech.com {
    device     /dev/drbd0;
    disk       /dev/sda6;
    address    10.0.0.2:7789;
    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.

3.3.3 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. This is no longer used as the NS-Link 5.16 firmware is now installed directly on the DeviceMasters. There is a line for each of the Devicemasters the Omega TNPP

router 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.

3.3.4 Digi Etherlite

The Digi Etherlite is another ethernet attached serial server supported for clustered (or non-clustered) systems. The Digi Etherlite is configured for DHCP out of the box and uses a 10baseT connection to the ethernet network. If you wish to leave the Digi configured for DHCP make sure that you enter the Digi's MAC address in your DHCP server to reserve the same IP address. Otherwise the TNPP-LX servers may not be able to find the Digi boxes if their IP address changes.

Type the following to install the Digi Etherlite Realports driver in Linux:

```
rpmbuild --rebuild \
http://support.harktech.com/dl/rhel5-x86_64/dgrp-1.9-17.src.rpm
rpm -ivh /usr/src/redhat/RPMS/x86_64/dgrp-1.9-17.x86_64.rpm
```

The above example shows the commands for building and installing on CentOS 5 64-bit version. For 32-bit version replace x86_64 with i386. If you are using Centos 4 replace rhel5 with rhel4.

Next we need to configure the Digi boxes. unitnumber is the Digi box number starting at 0, ip.addr is the IP address of the Digi box, and numports is the number of ports it has. For example, a Digi Etherlite 32 has 32 ports. Type the following line, once for each Digi box, setting the ip.addr and numports appropriately and incrementing the number after 'init':

```
dgrp_cfg_node -v -v init {unitnumber} {ip.addr} {numports}
```

For example, if you had two Digi Etherlite 32:

```
dgrp_cfg_node -v -v init DA 10.1.1.1 32
dgrp_cfg_node -v -v init DB 10.1.1.2 32
```

In the above examples make sure that you use upper-case letters for the unit ID (the parameter right after init). We recommend that you use the letter D followed by an incrementing letter for the unit number. For example, if you had a third Digi Etherlite on the system it would be DC.

Now the Digi service can be started with `service dgrp_daemon start` and the service can be set to start automatically on bootup with `chkconfig dgrp_daemon on`.

If you have a firewall between the TNPP-LX servers and the Digi Etherlite boxes, make sure that port 771 is allowed.

Chapter 4

tnpp.ini

The tnpp.ini file consists of several sections defining the configuration for separate parts of the Omega TNPP router.

4.1 [settings]

KEY_TYPE	Type of license key used. Supported values are DEMO for a time-limited demo version, HASP for Aladdin HASP HL USB key, Dallas for Dallas 1-wire serial key, or MB for other licensed versions.
LICENSE_KEY	The software license key. Clustered systems will actually have two LICENSE_KEY lines. One for each system. Not used for HASP or DEMO licenses.
FEATURE_KEY	Feature license key. Not used for HASP or DEMO licenses.
TRAFFIC_INTERFACE	The name of the ethernet interface your customer traffic is received on. This is typically eth0.
RLIMIT_MSGQUEUE	The amount of memory to allocate for POSIX message queues. Human readable shortcuts are allowed here. For example, 8 megabytes can be abbreviated as 8M (instead of 8388608).

DROP_PRIVILEGES
: Drop privileges and run as tnpplx user. By default a user named tnpplx and a group hark are automatically added to the system configuration files. Set this field to 1 or Y to enable running as the tnpplx user instead of root. If with the dropped privileges you will still be able to open ports < 1024 on Linux systems. This uses the CAP_NET_BIND_SERVICE capability. Also, the user will automatically be added to the uucp and lock groups so that it can open serial ports. Most serial ports are created 660 as root:uucp. If yours aren't, you may need to setup udev rules to make sure the serial port group is uucp with rw permissions.

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 function calls)
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

4.2 [httpd]

LISTEN_PORT
: The TCP port number to use for the web admin interface. Typically 80.

DEBUG_LEVEL
: Sets the amount of debugging information logged to the debug directory for the httpd process.

USERNAME
: Username for web admin login authentication. This may be up to 16 characters.

PASSWORD
: Password for web admin login authentication. This may be up to 16 characters.

ROUTE_DEVICE_DROPDOWN
: Use a drop-down box to select the device in the route configuration. This is helpful to limit the selections to only ports that exist. This option is configurable because on very large systems the route configuration page could take much longer to display.

4.3 [rtview]

SCAN_INTERVAL
: 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.

4.4 [syspage]

LISTEN_PORT
: The TCP port number to listen for error mesages on. Typically 1250.

IGNORE_TIME
: Packets received older than this number of seconds are ignored. This is helpful to limit a runaway alarm condition.

DEBUG_LEVEL
: Sets the amount of debugging information logged to the debug directory for the syspage process.

SERIAL_PORT
: Send a copy of the alarm text out the specified serial port. Use the full serial port name such as /dev/ttyUSB0 or /dev/tty63.

SERIAL_BAUD
: The baud rate to use to send the alarm text. The parity and data bits should be set to None and 8 (N-8-1).

SERIAL_NEWLINE
: Type of newline to send after the alarm text. 0=No newline, 1=Carriage Return only, 2=Line Feed only, 3=CRLF.

4.5 [tnppd]

AFFINITY_MASK
: The CPU affinity for Symmetric Multiprocessor Processor (SMP) systems. This is typically 0 which allows the tnppd process to run on all processors.

DEBUG_LEVEL	Sets the amount of debugging information logged to the debug directory for the tnppd process. See the description in the "settings" section above.
MAX_QUEUE	The maximum number of packets in the TNPP queue.
QUEUE_PERCENT	Once MAX_QUEUE is reached don't re-enable until the queue falls below this percentage. Typically this is set to 90.
RLIMIT_NOFILE	Set the maximum number of files the process is allowed to open. The typical Linux maximum is 1024. TNPP-LX systems with large numbers of serial and/or network ports may need to increase this to 8192 or even 32768.
FAULT_OFF_INPUT	If no output routes available fault off the input port.
TNPP_LOGFILE	Specifies the TNPP billing log filename format. Take care that the fully expanded name does not exceed 80 characters. This field allows some variable substitution. For example, %Y is the 4-digit year. This field may contain directory components, but it should not start with a /. If path starts with a slash it will be stored in the absolute path and may not be replicated to the standby server in clustered systems. Leave this field blank to use the default billing log format which is: logs/%Y/%m-%d/tnpp.txt. The following is a list of some of the variables supported (man strftime for full list):

%a	abbreviated weekday name
%b	abbreviated month name
%d	day of month (01 to 31)
%H	2-digit hour using 24-hour clock (00 to 23)
%I	2-digit hour using 12-hour clock (01 to 12)
%m	month of year (01 to 12)
%M	2-digit minute (00 to 59)
%p	AM or PM (upper-case)
%P	am or pm (lower-case)
%S	seconds (00 to 61, 60-61 are leap-seconds)
%y	2-digit year (00 to 99)
%Y	4-digit year

TNPP_BILLING_FIELDS

List of tokens representing the fields to write to the billing logs. These tokens are case-sensitive. Do not include any spaces in this value. As of version 3.10 string fields may optionally be prefixed by a + or a -. These control how a string field is truncated if it exceeds the field length defined by TNPP_BILLING_FORMAT. String fields are R, t, P, o, e, and I. For example, if you are limited to only 4 characters for the Port, you will probably want the rightmost 4 characters of the port (as they are more unique than the first 4 characters of the port). This can be done by using +P instead of P (or -P). As of version 3.14 the source, destination, channel, zone, and priority may be prefixed with < to output the value before translation or > for after translation. By default incoming packets will be logged before translation and outgoing packets will be logged after translation.

R	remote IP address
r	status
y	year
m	month
d	day
h	hour
i	minute
s	second
t	message text
l	message length
P	port
o	TNPP source ID
e	TNPP destination ID
I	pager capcode for cap packets, or ID for ID packets
T	pager type
C	pager class
c	channel
z	zone
p	priority
B	block type

TNPP_BILLING_FORMAT	List of tokens representing the field widths for each of the TNPP_BILLING_FIELDS tokens. Each column starts with an upper-case X which may be followed by zero or more lower-case x to represent the width. For example, to specify a five character wide field use Xxxxx. All non-x characters are copied to the log entry as-is. For example, the time can be represented with Xx:Xx:Xx to output 12:40:03.
TAP_LOGFILE	Specifies the TAP billing log filename format. See TNPP_LOGFILE for a detailed description.
TAP_BILLING_FIELDS	List of tokens representing the fields to write to the billing logs. These tokens are case-sensitive. Do not include any spaces in this value.

R	remote IP address
r	status
y	year
m	month
d	day
h	hour
i	minute
s	second
t	message text
l	message length
P	port
I	pager ID

TAP_BILLING_FORMAT	List of tokens representing the field widths for each of the TAP_BILLING_FIELDS tokens. Each column starts with an upper-case X which may be followed by zero or more lower-case x to represent the width. For example, to specify a five character wide field use Xxxxx. All non-x characters are copied to the log entry as-is. For example, the time can be represented with Xx:Xx:Xx to give a display like 12:40:03.
TAP_PROMPT_PAGERID	ID Prompt for TAP manual mode. TAP manual mode is not recommended for customer use, but has been added to allow for easier testing. This field is typically something like: Pager ID?
TAP_PROMPT_MESSAGE	Message prompt for TAP manual mode. This field is typically something like: Message?
TAP_PROMPT_ACCEPTED	The text to send when the TAP manual mode message has been successfully accepted.

TAP_PROMPT_REJECTED	The text to send when the TAP manual mode message has been refused.
SNPP_SERVER	The SNPP server hostname or IP address to send messages received via the TAP protocol.
SNPP_PORT	The port number on the SNPP server to connect and send messages received via the TAP protocol. This is typically 444.
SNPP_MAXMSGLEN	The maximum number of characters allowed in the outgoing SNPP message. Acceptable values are 16 to 1024.
SNPP_LINKTEST	The number of seconds between SNPP link tests. Each thread configured for the TAP protocol will open a connection to the SNPP server and keep that connection open as much as possible to reduce the overhead required to send a message via SNPP. Acceptable values are 5 to 1800. This value must be shorter than the timeout setting on your SNPP server in order to keep the connection alive.

4.6 [route]

Route entries are in the following form:

Destination|Enabled|Description|Port|NewSource|NewDestination| NewInertia|NewChannel|NewZone|NewPriority

Each field is separated by a vertical bar (|) also known as a pipe symbol. The destination is the TNPP destination of the packet to be routed. Individual routes can be enabled or disabled by setting the enabled field to Y or N (also 1 or 0 is acceptable). Multiple routes can be specified for each destination. The Description field is informational only and can be left blank. The Port field specifies which logical port the packet is to be delivered. If the NewSource or NewDestination fields have a value those values are used when sending the packet to the destinations. To prevent the system from remapping the Inertia use a value of 0. The NewChannel and NewZone fields are ignored if the value is set to 64. The NewChannel and NewZone may be set to values from 0 to 63 to remap those fields to specified channel or zone. The NewPriority allows remapping of the priority flag. Set to 0 to disable the priority flag in the routed packets. For TNPP Extended Cap packets a value of 1 to 31 is allowed. See the TNPP 3.8.1 Protocol Guide for more information. Set the NewPriority field to 32 to disable priority remapping.

For example:

```
E002|1|Test port|port4|||0|64|64|32
```

4.7 [alarm]

The alarm section is also specified like the route section. Its fields are as follows:

Name|Enabled|Severity|Protocol|Host|Port|Recipient|InitTimeout|SecTimeout

The Name is a descriptive name and must be specified. Each alarm can be enabled or disabled by setting the Enabled field. The Severity is the severity level at which this alarm will be sent. Severity level 63 and below is informational, 64 to 127 is a warning, and 128 and above are errors. Typically alarms are set to severity 128, but if you want a copy of alarms in your email, you might choose severity 64. Protocol is the protocol to send the alarm. Currently the SMTP and SNPP protocols are supported. The Host is the IP address or hostname of the server to send the alarm to and the Port is the TCP port number to use. Typically the Port number will be 25 for email or 444 for SNPP. For email alarms the recipient is the full email address. For SNPP specify the pager ID. The InitTimeout is the amount of time in milliseconds to wait for data from the remote. The SecTimeout is the amount of time in milliseconds to wait for additional data after each successful read from the remote.

For example:

```
Support|1|128|SMTP|mail.example.com|25|support@example.com|45000|5000
Pager|1|128|SNPP|snpp.example.com|444|8435551212|30000|1000
```

4.8 [port...]

This is where each logical port is defined. There are several fields which control different aspects of the port and its settings. The following is a list of the port fields and their function:

DESCRIPTION	An informational description for this port.
DEVICE	The actual device used by this port. For serial ports this will be the actual device file (e.g. /dev/ttySI0). For TCP ports this will be TCP: followed by the TCP port to listen on (e.g. TCP:10000).
ENABLED	Enable or disable the port.
DEBUG_LEVEL	A port specific debug level. This allows large systems to run without debugging to save on the large amount of data written to the drive and enable debugging on specific ports to troubleshoot customer issues.

TNPP_ID
: The TNPP ID to send in init packets. This is a 4-digit hexadecimal value and should be padded on the left with zeros. Also upper-case hexadecimal letters should be used. For example, 03FA.

BACKUP_DEVICE
: Specify an alternate port if this port faults-off for any reason. The format is the same as the DEVICE field. For example, serial ports will be in the form of /dev/ttySI0 or /dev/ttyUSB0, etc. Network ports will be in the form of TCP:[portnum].

OPTION
: Protocol options. This where non-standard TNPP options would be specified such as ISI link tests and other vendor specific modifications. Add the numbers listed next to the option for the final value. For example, to communicate with a CommOne Client or Gateway add 8+16+32 for a total value of 56. The web admin interface will have these options as checkboxes so you can easily select the options you want.

1	Transparent CRC
2	Simplex
4	Hark ISI
8	CommOne
16	CommOne Ack Please
32	CommOne Ack Back
128	No Init Packet
256	RTS ATNP
536870912	Encrypt TCP session

DIRECTION
: 1=input, 2=output, 3=bi-directional. Most ports will be bi-directional. If you need to support simplex ports. This is where you would define if it is simplex input or simplex output.

INERTIA
: The inertia to use in init packets.

SIMPLEX_TRANSMITS
: The number of times to transmit packets on outgoing simplex ports. Because there is no acknowledge (positive or negative) on simplex links a method was devised to retransmit packets a set number of times with the hope that at least one of the packets will get through. This can be done because the same serial number is used for each retransmit which the receiving TNPP device knows to ignore if the serial number matches one it recently received.

HOST	Host name to connect to. This is used when the Omega TNPP router will be used as a client to connect to a remote server. Leave this field blank to allow the Omega to act as the server and listen for connections from clients.
PORT	The TCP port number to listen on for when the Omega is a server, or the TCP port number to connect to when the Omega is acting as a client and there is a name or IP address in the HOST field to connect to.
SOCK_DOMAIN	The socket domain. Currently the TNPP-LX only supports the INET domain.
SOCK_TYPE	This may be set to either UDP or TCP. Typically this will be TCP unless some third party TNPP over net client requires UDP.
SOCK_ADDR	Allows the binding of specific IP addresses. This is typically not used and should be left blank or set to 0. In systems with multiple ethernet interfaces it is possible to enter the IP address of the ethernet interface on which to listen. Entering 0 or leaving blank will allow the Omega to listen on all ethernet interfaces. This can be used for server or client connections.
SOCK_PORT	Allows the binding of specific outgoing port. This is typically not used and should be left blank or set to 0. Some TNPP over net routers may require client connections to be from a specific port. Set this value to that port. Note: Each TNPP logical port must use a unique outgoing TCP port.
USERNAME	Some TNPP over net servers or clients require a username.
PASSWORD	The password to use for the above username.
MODEM_TYPE	0=NONE, 1=ANSWER, or 2=DIAL. Set to NONE for direct RS-232 connections. Set to ANSWER to answer incoming calls or DIAL to dial a remote paging terminal.
MODEM_NUMBER	The telephone number to dial if MODEM_TYPE is set to DIAL.
MODEM_INIT1	The first init string to send to the modem.
MODEM_INIT2	The second init string to send to the modem if the entire string can't fit into the first string or if your modem requires the init string to be broken in two.

BAUD	The baud rate of the serial port.
PARITY	The parity of the serial port. The TNPP standard is to use no parity (N). For TAP, even parity (E) should be used.
DATABITS	The number of data bits for the serial port. The TNPP standard is to use 8 data bits. For TAP, 7 data bits should be used.
STOPBITS	The number of stop bits for the serial port. This will almost always be 1.
PACKET_SIZE	Originally the TNPP specification only allowed for 1024 bytes packets. Recent versions now support 4096 byte packets. The Omega TNPP router supports both. However, there is no defined method for determining if a remote device will support 4096 byte packets, so most systems still use 1024. The default value is 1024.
TICT	The TNPP inter-character timer. The amount of time once we receive a character we will wait for the next character. This is specified in milliseconds. The default is 2000.
TNRI	The TNPP no response idle timer. The amount of time after sending a packet before waiting for a reponse times out. There is also a TNRB timer in TNPP, but we don't use it because our transmitter is never busy. The Omega sends an entire packet at once and will not look for an incoming character until it is done. Hence the transmitter is never busy. The default value for TNRI is 10000 milliseconds.
TNRE	TNPP no response ENQ. The amount of time to wait for a response after sending and ENQ (link test). The default value is 10000 milliseconds.
THOLD	The amount of time in the future to reschedule the packet when an RS is received. The default value is 10000 milliseconds.
TIDLE	If there is no activity on this port in TIDLE milliseconds a link test is sent. The default value is 60000.
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.
ALLOW_SOURCE	ALL or a comma separated list of TNPP source ID's to allow. Default is ALL. If you wish to specify allowed sources, a maximum of 32 sources per port are allowed.
DENY_SOURCE	NONE or a comma separated list of TNPP source ID's to deny. Default is NONE. To use the DENY_SOURCE list, ALLOW_SOURCE must be set to ALL. A maximum of 32 sources to be denied are support per port.
BLOCK_TYPE	ALLOW:type or DENY:type where type is one or more of CAP, ID, EXTCAP, or COMMAND. See description following this section on how the ALLOW and DENY specification work. The default is to allow all block types.
PAGE_TYPE	Similar to BLOCK_TYPE except refers to the page type. The type is one or more of P512, P1200, P2400, GOLAY, FLEX, 56TONE, 2TONE, RDS, DTMF, NECD3. This default is to allow all page types.
PAGE_CLASS	Similar to PAGE_TYPE except refers to the page class. The type is one or more of NUMERIC, ALPHA. The default is to allow all page class.
BATCH_COUNT	Number of packets to batch before dialing out on a MODEM_TYPE=DIAL port. If BATCH_COUNT is 0 the modem will immediately be dialed out and doesn't time out. If the remote end disconnects it will automatically be redialed.
BATCH_TIME	The amount of time in seconds to hold the modem out-dial connection after sending all pending packets. This setting is designed to minimize dialing out in case there will be another packet to send soon.
LOG_DUPS	Specify whether or not to log duplicate TNPP packets in the billing logs. Default is N.
LOG_TYPE	Log incoming packets, outgoing packets, or both. Allowable values are OFF, IN, OUT, or BOTH. Numerical values are also supported: 0=Off, 1=In, 2=Out, 3=Both. The default is OFF. Make sure to enable this for each port that you wish to capture billing logs.

Three of the above fields, BLOCK_TYPE, PAGE_TYPE, and PAGE_CLASS have an ALLOW and DENY option. Most systems will probably use ALLOW:ALL to accept all packets, but some installations may wish more control over the packets going through the router. This can be accomplished in a couple of ways. First, you can specify which packets you want to allow. This will block all non-matching packets. Second, you may wish to only block certain packets and allow everything else through.

To handle the first situation just create ALLOW lines. For example to only allow alphanumeric POCSAG 512, and POCSAG 2400 cap packets the following settings would be used:

```
BLOCK_TYPE=ALLOW:CAP
PAGE_TYPE=ALLOW:P512,P2400
PAGE_CLASS=ALLOW:ALPHA
```

The following is an example of the second situation where you want to accept any packets except COMMAND packets:

```
BLOCK_TYPE=DENY:COMMAND
PAGE_TYPE=ALLOW:ALL
PAGE_CLASS=ALLOW:ALL
```

If a DENY is specified and there is a DENY match, the packet is rejected with a CANcel. If there are DENY that don't match and ALLOW that match the packet is accepted. If there are only ALLOW and the packet is not matched, the packet is rejected with a CANcel. If there are no ALLOW entries and no DENY entries the packet is allowed. If there are only DENY entries and no match, the packet is allowed.

4.9 Example tnpp.ini

```
[settings]
KEY_TYPE=/dev/ttyS1
LICENSE_KEY=[insert license key here]
LICENSE_KEY=[license key for standby server]
DEBUG_LEVEL=65535

[httpd]
LISTEN_PORT=8080
DEBUG_LEVEL=0
```

```
USERNAME=[up to 16 char username]
PASSWORD=[up to 16 char password]

[rtview]
SCAN_INTERVAL=500

[syspage]
LISTEN_PORT=1250
IGNORE_TIME=120
DEBUG_LEVEL=0
INIT_TIMEOUT=30000
SEC_TIMEOUT=1000

[tnppd]
AFFINITY_MASK=15
DEBUG_LEVEL=0
MAX_QUEUE_ENTRIES=32
QUEUE_PERCENTAGE=98
FAULTOFF_INPUT=N
TNPP_BILLING_FIELDS=hisoerRITCczPlt
TNPP_BILLING_FORMAT=Xx:Xx:Xx Xxxx Xxxx X Xxxxxxxxxxxxxx Xxxxxxxxx X X \
X X Xxxxxxxxxxxxxxxxxxx Xxx X
TAP_BILLING_FIELDS=hisrRIPlt
TAP_BILLING_FORMAT=Xx:Xx:Xx X Xxxxxxxxxxxxxx Xxxxxxxxx \
Xxxxxxxxxxxxxxxxxxx Xxx X
TAP_IDPROMPT=Pager ID?
TAP_MESSAGEPROMPT=Message?
TAP_SUCCESSPROMPT=Message sent.
TAP_FAILPROMPT=Send failed.
SNPP_SERVER=snpp.pagingcentral.com
SNPP_PORT=444
SNPP_MAXMSGLEN=240
SNPP_LINKTEST=20

[alarm]
test|1|128|smtp|10.100.1.253|25|support@harktech.com

[route]
# DEST|EN|DESC|PORT|NEWSRC|NEWDEST|NEWINERTIA|NEWCHAN|NEWZONE|NEWPRI
B00F|1|Test route|port1|||0|64|64|32
#E000|1|Test route|port1|||3|64|64|32
#E000|1|Test route|port1||D002|3|64|64|32
E000|1|Test route|port2||D002|3|64|64|32
E000|1|Test route|port3||D002|3|64|64|32
E000|1|Test route|port4||D002|3|64|64|32
```

```
# Example TNPP serial port

[port1]
DESCRIPTION=Com port 1
DEVICE=/dev/tty_dgrp_1_0
BACKUP_DEVICE=/dev/ttyUSB0
ENABLED=1
TNPP_ID=A000
PROTOCOL=TNPP
OPTION=0
DIRECTION=3
INERTIA=2
MODEM_TYPE=NONE
BAUD=9600
PARITY=N
DATABITS=8
STOPBITS=1
PACKET_SIZE=1024
TICT=2000
TNRI=10000
TNRE=10000
THOLD=10000
TIDLE=60000
CRETRYMAX=6
CHOLDMAX=24
CENQMAX=6
ALLOW_SOURCE=ALL
BLOCK_TYPE=ALLOW:ALL
PAGE_TYPE=ALLOW:ALL
PAGE_CLASS=ALLOW:ALL
BATCH_COUNT=0
BATCH_TIME=5
LOG_DUPS=Y
LOG_TYPE=BOTH

# Example TAP serial port

[port2]
DESCRIPTION=Com port 2
DEVICE=/dev/tty_dgrp_1_1
ENABLED=1
PROTOCOL=TAP
OPTION=0
DIRECTION=IN
MODEM_TYPE=NONE
BAUD=9600
```

```
PARITY=E
DATABITS=7
STOPBITS=1

# Example TNPP network port

[port10]
DESCRIPTION=TCP 10000
DEVICE=tcp:10000
ENABLED=1
TNPP_ID=F001
PROTOCOL=TNPP
OPTION=0
DIRECTION=3
INERTIA=2
HOST=
PORT=10000
SOCK_DOMAIN=INET
SOCK_TYPE=TCP
SOCK_ADDR=
SOCK_PORT=
PACKET_SIZE=1024
TICT=2000
TNRI=10000
TNRE=10000
THOLD=10000
TIDLE=60000
CRETRYMAX=6
CHOLDMAX=24
CENQMAX=6
ALLOW_SOURCE=ALL
BLOCK_TYPE=ALLOW:ALL
PAGE_TYPE=ALLOW:ALL
PAGE_CLASS=ALLOW:ALL
LOG_DUPS=N
LOG_TYPE=BOTH

# Example TAP network port

[port11]
DESCRIPTION=TCP 10001
DEVICE=tcp:10001
HOST=
PORT=10001
ENABLED=Y
PROTOCOL=TAP
```

```
OPTION=0
DIRECTION=IN

# Example of port using TNPP defaults

[port12]
DESCRIPTION=TCP 10002
DEVICE=tcp:10002
HOST=
PORT=10002
ENABLED=1
TNPP_ID=F001
PROTOCOL=TNPP
OPTION=0
DIRECTION=3
INERTIA=2
LOG_DUPS=N
LOG_TYPE=IN

# end of tnpp.ini
```

Chapter 5

Program Descriptions

The TNPP router runs from the /opt/tnpplx directory.

5.1 bin

This directory contains the utilities and maintenance programs. These are commands and utilities you will use from the command line after logging in to view stats and other functions.

5.1.1 rtview

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

5.1.2 showlog

Displays the billing log entries as they are added to the billing log file. When first started showlog will automatically go to the end of the file and start displaying new entries as they are added. To view the TNPP logs type:

```
showlog tnpp
```

5.1.3 oservice

The oservice program can list the running onixd processes or start and stop them. To list the current services and their status type the following:

```
oservice list
```

To stop a service, for example httpd, type:

```
oservice httpd stop
```

To start a service that is not running, for example httpd, type:

```
oservice httpd start
```

5.1.4 sptest

The sptest program is for sending alarms via the syspage server. By default the sptest program will send a test alarm. 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"
```

5.2 sbin

The server binaries directory. This is where the system server programs are stored. The system server programs start automatically when the system boots. It is not necessary to login for these programs to start.

5.2.1 httpd

The web admin server. Allows the tnpp.ini file to be maintained from a web page. See the "Web Administrative Interface" chapter for more information.

5.2.2 onixd

The main process starter and monitor. Onixd will automatically start the syspage, httpd, and tnppd servers and monitor them. If for some reason one of them should exit, onixd will send an alarm and automatically restart the process.

5.2.3 syspage

The system alarm paging server. Syspage is configured in the [syspage] and [alarm] sections in tnpp.ini. See the "tnpp.ini" chapter for more information.

5.2.4 tnppd

The main TNPP router program. This program is responsible for starting all of the logical ports defined in tnpp.ini. It is multithreaded and starts a thread for each port. As new ports are added to the tnpp.ini file, tnppd will automatically start a thread for them. There is no need to restart the program when adding new ports. As of version 3.5 the tnppd program also supports TAP connections. TAP connections are supported over serial port connections or TCP/IP connections. A port may be setup for the TAP protocol or TNPP protocol, but not both.

When using the TAP protocol the port will automatically connect to the SNPP server and send RESE to keep the connection alive. This allows us to check to see if the ID is accepted before accepting the packet from the TAP client. The ID is sent to the SNPP server exactly as it is received. We don't strip dashes or prefix/strip any digits. If the SNPP server rejects the ID, the Omega will send pack the proper TAP reject message (RS in case of automatic TAP). We do support manual mode TAP for testing only! It is not intended for customers to actually use and is included only to help with easily testing connections from a telnet client or terminal emulation software.

Chapter 6

Web Administrative Interface

The Omega TNPP router includes a web-based interface for maintenance of the tnpp.ini file. The tnpp.ini file is a plain text file and can be edited with an included text editor such as vi, however we also include this web interface to make certain maintenance operations easier. To access the web admin interface enter the url for the TNPP-LX. Please see the "tnpp.ini" chapter for more information on the individual fields which are maintained through this web interface.

6.1 Configuration

6.1.1 Port number

Based on your settings you may need to enter a special url. For example, if you change the LISTEN_PORT in the [httpd] section of tnpp.ini from the default of 80 to 8080, you would need to use a url such as: http://tnpp.example.com:8080 . This port will need to be added to the firewall configuration. See the "Firewall and Port Security section".

6.1.2 Login authentication

Login authentication is now available. To enable login authentication specify a USERNAME and PASSWORD in the [httpd] section of tnpp.ini. If you change either of these values using the web admin interface you will need to reload the page. Simply clicking refresh or one of the buttons on the page will not work. Once logged in you will not need to login again unless you close your browser. If either the USERNAME or PASSWORD fields are blank, login authentication is disabled.

6.1.3 Encryption

If you are accessing the web admin interface you may want to look into using SSL to encrypt the session. This can be done with the stunnel program. Here is a sample from the stunnel configuration file in /etc/stunnel/stunnel.conf:

```
[https]
accept  = 443
connect = localhost:80
TIMEOUTclose = 0
```

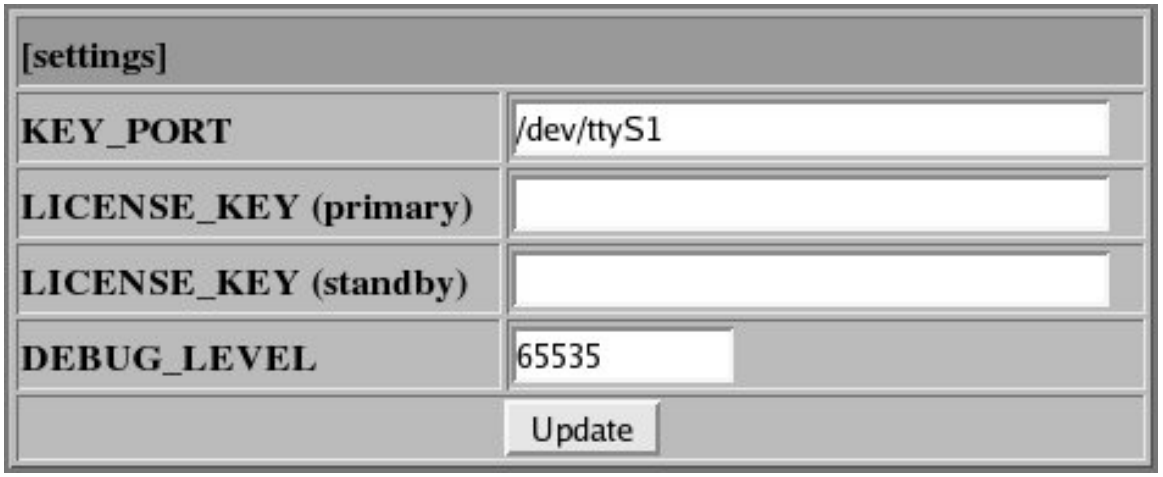
Just type stunnel to start the program and allow https connections to the web server. To stop stunnel, type `killall stunnel`.

6.2 Main page

The following is a screen shot of the main web page. The buttons represent the section of the tnpp.ini file to maintain. For example, click settings to edit the [settings] section of tnpp.ini.

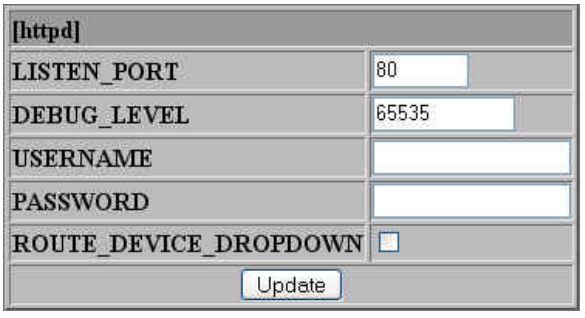
6.3 Settings

Allows the maintenance of the settings section.



6.4 httpd

Allows the maintenance of the httpd section.

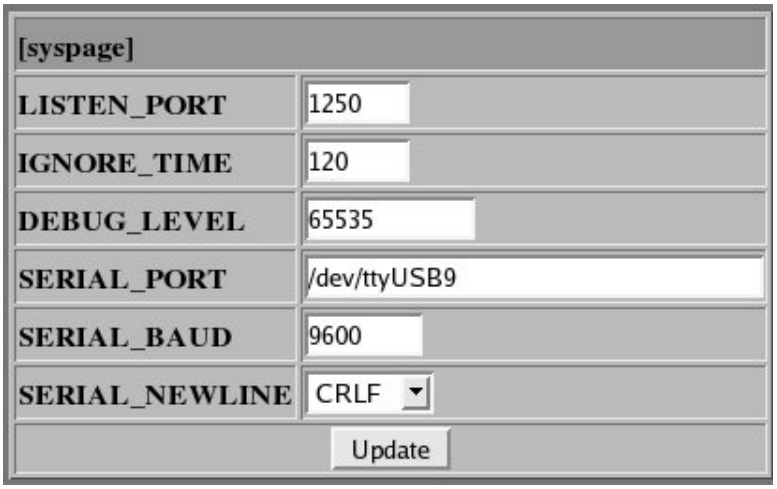


6.5 rtview

Allows setting of the rtview settings.

6.6 syspage

Allows the maintenance of the syspage section.



[syspage]	
LISTEN_PORT	1250
IGNORE_TIME	120
DEBUG_LEVEL	65535
SERIAL_PORT	/dev/ttyUSB9
SERIAL_BAUD	9600
SERIAL_NEWLINE	CRLF
	Update

6.7 tnppd

Allows the maintenance of the tnppd section.

[tnppd]	
AFFINITY_MASK	0
DEBUG_LEVEL	65535
FAULTOFF_INPUT	☐
MAX_QUEUE	1000
QUEUE_PERCENT	90
TNPP_LOGFILE	
TNPP_BILLING_FIELDS	hisoerRITCcz+Plt
TNPP_BILLING_FORMAT	XcXxXx Xxxx Xxxx X Xxxxxxxxxxxxxx Xxxxxxxxx XXXX Xxxx Xxx X
TAP_LOGFILE	
TAP_BILLING_FIELDS	hisrRIPlt
TAP_BILLING_FORMAT	XcXxXx X Xxxxxxxxxxxxxx Xxxxxxxxx Xxxxxxxxxxxxxxxxxx Xxx X
TAP_PROMPT_PAGERID	Pager ID?
TAP_PROMPT_MESSAGE	Message?
TAP_PROMPT_ACCEPTED	Message sent.
TAP_PROMPT_REJECTED	Send failed.
SNPP_SERVER	10.100.1.251
SNPP_PORT	444
SNPP_MAXMSGLEN (16-1024)	240
SNPP_LINKTEST (5-1800 seconds)	20
	Update

6.8 port

Allows the maintenance of the port section. The port settings have been split into two pages due to the very long load time with hundreds of ports. The first page lists all of the ports along with some of their settings. Scroll this page until you find the port you are looking for and click the "Edit" or "Delete" button next to it. The Delete button will delete the port. It does not ask for confirmation so make sure you have the correct port before deleting it. The Edit button will display the port on a new web page with the settings in editable fields. Once you are done, click Update to save your changes. The following is an example of the main port list page:

Port	Device	Enabled	Description	Protocol	TNPP ID	Connection	
1	/dev/ttyUSB0	Yes	test	TNPP	A001	9600 N-8-1	Edit Delete
2	/dev/ttyUSB2	Yes	test	TAP		9600 E-7-1	Edit Delete
10	TCP10000	Yes	tcp test	TNPP	B000	[server]:10000	Edit Delete
11	TCP10001	Yes	tcp test	TAP		[server]:10001	Edit Delete
						New port	

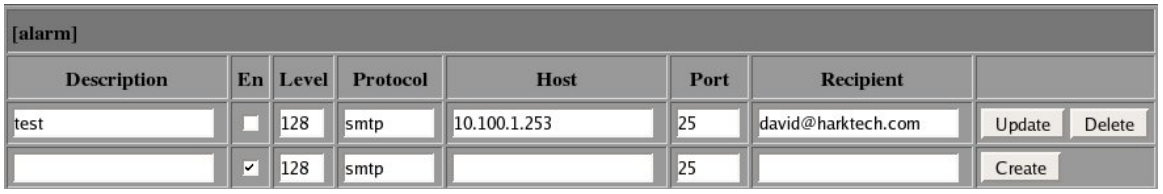
The first column is the logical port number. See the "[port]" section for description of the Device, Enabled, Description, and TNPP ID fields. The Connection column will have different information depending on the type of port. A TCP client port will have a host name or IP address followed by a colon and port number. A TCP server port will have [server] followed by : and the port number. A serial port will have a modem number if the port is a modem dial out port, followed by the baud rate, parity, data bits and stop bits.

To add a new port click the "New port" button at the bottom of the screen. If you have many ports you may need to scroll the web page to see the bottom. Some web browsers allow you to press <End> or <Ctrl><End> to go to the bottom of the web page. Click Edit on one of the ports (in this example port 2) to edit the port settings.

[port 1]	
DEVICE	/dev/ttyUSB0
ENABLED	☑
DESC	test
DEBUG_LEVEL	65535
BACKUP_DEVICE	
DEPENDS_ON	
TNPP_ID	A001
PROTOCOL	TNPP
OPTION	☐ Transparent CRC ☐ Simplex ☐ Hark ISI ☐ CommOne ☐ CommOne AckPlease ☐ CommOne AckingBack ☐ Don't send init packet ☐ Encrypt
DIRECTION	Bi-directional
INERTIA	2
USERNAME	
PASSWORD	
MODEM	None (direct)
BAUD (P-D-S)	9600 None 8 1
PACKET_SIZE	1024
TICT	2000
TNRI	10000
TNRE	10000
THOLD	10000
TIDLE	10000
CRETRYMAX	6
CHOLDMAX	24
CENQMAX	6
BATCH_COUNT	0
BATCH_TIME	0
ALLOW_SOURCE	ALL
DENY_SOURCE	NONE
BLOCK_TYPE (allow)	ALL
PAGE_TYPE (allow)	ALL
PAGE_CLASS (allow)	ALL
LOG_DUPS	☐
LOG_TYPE	Input and Output

6.9 alarm

Allows the maintenance of the alarm section. The alarm page works a little different than the port page. All of the alarms are displayed in an editable form on one page. To make changes to a specific alarm edit the fields and click the update button next to it. You can only update one line at a time. If you modify more than one line and click update, only the line you click update will be modified. You may also create new alarms by entering the information on the last line with the blank fields (some default information is already filled in) and click Create.

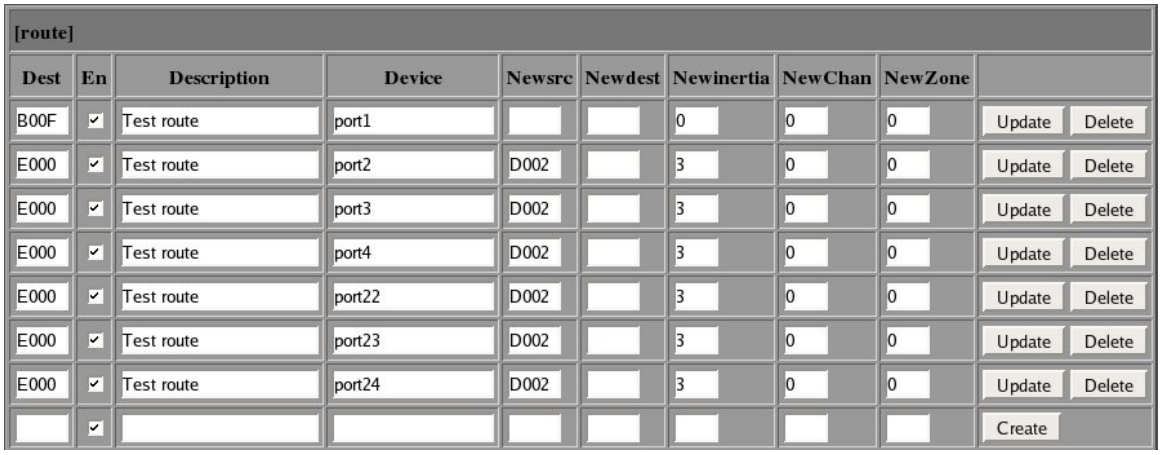


[alarm]

Description	En	Level	Protocol	Host	Port	Recipient	
test	☐	128	smtp	10.100.1.253	25	david@harktech.com	Update Delete
	☑	128	smtp		25		Create

6.10 route

Allows the maintenance of the route section. The route page works like the alarm page. All of the routes are displayed in an editable form on one page. To make changes to a specific route edit the fields and click the update button next to it. You can only update one line at a time. If you modify more than one line and click update, only the line you click update will be modified. You may also create new routes by entering the information on the last line with the blank fields (some default information may already be filled in) and click Create.



[route]

Dest	En	Description	Device	Newsrc	Newdest	Newinertia	NewChan	NewZone	
B00F	☑	Test route	port1			0	0	0	Update Delete
E000	☑	Test route	port2	D002		3	0	0	Update Delete
E000	☑	Test route	port3	D002		3	0	0	Update Delete
E000	☑	Test route	port4	D002		3	0	0	Update Delete
E000	☑	Test route	port22	D002		3	0	0	Update Delete
E000	☑	Test route	port23	D002		3	0	0	Update Delete
E000	☑	Test route	port24	D002		3	0	0	Update Delete
	☑								Create

Chapter 7

Billing

Billing information is stored in the /opt/tnpplx/logs directory. These logs are further broken down by year and month/day to help keep the logs managable. For example, April 14th, 2006's billing logs are stored in the /opt/tnpplx/logs/2006/04-14 directory. Messages received with the TNPP protocol will be stored in tnpp.txt and messages received with the TAP protocol will be stored in tap.txt. The format of these files is configurable. See the BILLING_FIELDS and BILLING_FORMAT settings in the tnpp.ini chapter.

7.1 Status field

The following are the status field values for TAP connections:

F	Failed (Automatic mode)
S	Success (Automatic mode)
I	Invalid ID
T	Timeout
C	Bad Checksum
B	Bad block
f	Failed (Manual mode)
s	Success (Manual mode)

The following are the status field values for TNPP connections:

N	Outgoing packet NAKed
A	Outgoing packet ACKed
C	Outgoing packet CANed
R	Outgoing packet RSed
n	Incoming packet NAKed
f	Incoming packet filtered (blocked)
a	Incoming packet ACKed
c	Incoming packet CANed
r	Incoming packet RSed
T	Timeout
F	No route and FaultOffInput enabled
2	Duplicate serial number

Chapter 8

Troubleshooting

The Omega TNPP Router can be configured to keep very detailed logs for troubleshooting customer or connectivity issues. The default debug level should be set fairly low as the debug logs can grow to very large sizes. The logs are also retained for several days. There is a configurable cron job which will remove the files after a configurable number of days. The default is 7 days. These logs are stored in the /var/opt/tnpplx/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/tnpplx/debug/2006-04-14. Inside this sub-directory there are files for each thread of each program running. For example, the first tnpp port will be in a file called tnppd000_ttyx.dbg. The 000 is the first thread (threads use 0-based numbering), the ttyx is the name of the device. In the case of serial ports it will normally be tty something. For TCP ports it will be based on the name entered for DEVICE in the port settings.

8.1 Operating system

8.1.1 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?

8.1.2 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 network TAP/TNPP connections, 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
```

8.2 Application

8.2.1 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 serial port (Comm) routines and the Net functions handle network connections. Other lines are also logged that show additional information.

8.2.2 Alarms

Application alarms are sent to the syspage server running on the Omega TNPP router. 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/tnpplx/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, SNPP, or WCTP protocols.

8.2.3 Message queues

The TNPP-LX uses POSIX Message Queues for routing packets between different TNPP ports. 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.

8.3 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 9

Maintenance

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

9.1 Backups

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 tnpplx 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/tnpplx
```

If this returns more than 650000 the billing logs may need to be archived. This can be done a few different ways. If you have an entire years worth of billing logs you may want to zip the entire year. For example, to zip up the entire year of 2005 type the following:

```
cd /opt/tnpplx/logs
zip -r 2005.zip 2005
```

You can verify the zip file with:

```
unzip -v 2005.zip
```

If no errors are reported you may delete the 2005 directory with the following:

```
rm -rf 2005
```

To zip a single month, cd into the year directory with the following:

```
cd /opt/tnpplx/logs/2006
zip -r jan.zip 01-??
```

Again verify the zip file as described above and remove the 01-?? directories with the following command:

```
rm -rf 01-??
```

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

```
mkisofs -R /opt/tnpplx | 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:
```

9.2 Daily maintenance

None at this time

9.3 Weekly maintenance

9.3.1 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.

9.4 Monthly maintenance

9.4.1 Filters

Depending on the installation site, the filter in the front of the Omega TNPP Router may need to be washed (or vacuumed). To do this perform the following steps:

- 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.
- Wash the filter using plain water.
- Set filter on paper towels and let the filter air-dry.
- Make sure the filter is completely dry before reinstalling.
- Reinstall filter by reversing the steps used to remove it.

Chapter 10

Change summary

Along with some minor changes and bugfixes in most versions the following major changes have been made:

10.1 Changes from 3.14 to 3.15

- support dropping privileges
- added DROP_PRIVILEGES configuration item
- added RLIMIT_NOFILE configuration item
- added RLIMIT_MSGQUEUE configuration item
- change from ctree message queues to posix message queues like on the IMG-LX (make sure RLIMIT_MSGQUEUE is at least # threads * 8.5K * # queue entries)
- added TRAFFIC_INTERFACE config item for non key-based license and to get ip settings from traffic interface instead of first non-loopback interface found
- syspage network read timeouts are now configurable
- now rechecks license key after any error (10 times 5 minutes apart)
- bugfix-CGLE multiple block in packet responses
- log_packet now strips control characters from message data
- process_packet now supports require link resp (EOT) for more strict following of TNPP protocol (default is any good packet or remote link test request will satisfy our outgoing link test)
- bugfix-process_packet don't set state to 2 on receive ACK unless state > 2

10.2 Changes from 3.13 to 3.14

- billing logs now support < and > prefix to specify whether the pre-translation or post-translation values are to be used for source,dest,chan,zone,priority
- bugfix-input log is now pre-translation by default
- added billing token n for inertia
- added billing token p for priority
- httpd changed from multi-threaded to multi-process
- syspage changed from multi-threaded to multi-process

10.3 Changes from 3.12 to 3.13

- added ability to remap priority in the route table

10.4 Changes from 3.11 to 3.12

- bugfix-syspage/sthread close debug file handle when finished with it
- syspage now sends Message-Id and Date headers to help spamassasin not think alarms are spam
- if read an SOH from remote but don't receive ETX and there is a read timeout from remote, fault-off the port

10.5 Changes from 3.10 to 3.11

- now uses short cap for logging
- bugfix-perform channel/zone remapping on all blocks in a packet
- now supports RTS ATNP protocol

10.6 Changes from 3.9 to 3.10

- restore previous XON operation, caused problem with Glenayre serial TNPP being passed transparently over the Internet
- move log_type and log_dups from tnpp settings to port settings
- change parse_logtype to allow NONE in addition to OFF

- changes to log_type and log_dups now take effect immediately
- bugfix-if EOT received when sending init packet, send init packet again
- bugfix-log incoming packets was broke in 3.7
- billing now support logging rightmost characters of field for values that overflow field widths
- bugfix-port recovered alarm not sent if remote TCP connection was closed normally

10.7 Changes from 3.8 to 3.9

- bugfix-if packet size < 4096 and more than packet size bytes received without getting an ETX thread would loop endlessly
- bugfix-queue_packet allow newchan and newzone to be 63
- rtview allow F6 and F7 to stop/start START and FAULTOFF threads

10.8 Changes from 3.7 to 3.8

- check for modem hangup more often in initialization routines
- support custom filenames for tap and tnpp billing log file names
- add deny source support to complement already existing allow source

10.9 Changes from 3.6 to 3.7

- support debug files larger than 2 gigabytes
- support setting sockdomain, socktype, and sockaddr
- bugfix-more changes for alarm array/route allocation in web admin

10.10 Changes from 3.5 to 3.6

- created onixd to start the TNPP-LX processes and monitor them, automatically restarting them if they exit for any reason
- httpd limit numeric field ranges for fields with limits
- support Aladdin USB hardware key

- httpd limit channel and zone to 0 to 64
- created oservice to start/stop/list TNPP-LX services
- httpd changed from fork to multi-threaded model
- httpd now supports optionally dropping down a list of devices for routes
- TAP and TNPP Internet connections now support encryption from other TNPP-LX servers or from Hark ISI remotes

10.11 Changes from 3.4 to 3.5

- httpd now supports a username and password for logging in
- support TAP input (serial and network) and send directly to an SNPP server
- support TAP manual mode for testing
- httpd use lighter shade of grey
- httpd change main menu link to button for better visibility
- now automatically sets higher resource limits automatically

10.12 Changes from 3.3 to 3.4

- rtview use SHIFT-DEL to clear all counters
- don't queue packet out same device it came in on
- bugfix-httpd show_page had newsrc and newdest reversed

10.13 Changes from 3.2 to 3.3

- rtview use CTRL-R to redraw screen
- rtview use delete key to clear counters
- rtview scan time now configurable
- fixed bugs in code to act as a CommOne server
- fixed bug which prevented more than 5 alarm entries to be created in the web admin

10.14 Changes from 3.1 to 3.2

- Support acting as a CommOne server in addition to acting as a CommOne client

10.15 Changes from 3.0 to 3.1

- Debug logs moved from /opt/tnpplx to /var/opt/tnpplx
- New web admin to support using tnpp.ini instead of databases
- Added TNPP batching for dialup connections (batchtime and batchcount)

Chapter 11

Warranty Information

WARRANTIES

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

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

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

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

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

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

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

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

DISCLAIMER OF WARRANTIES

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

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

BREACH OF AGREEMENT

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

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

ALTERATIONS AND CHANGES

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

PROPOSAL GOOD FOR THIRTY (30) DAYS

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

AGREEMENT SUBJECT TO APPROVAL BY MANAGEMENT

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

ACTS BEYOND HARK'S CONTROL

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

SECURITY AGREEMENT

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

BAD CHECKS & C.O.D.

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

RETURNS

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

HANDLING/RESTOCKING CHARGE

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

EQUIPMENT PACKING

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

DO NOT PACK HARK EQUIPMENT IN STYROFOAM PEANUTS ONLY

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

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

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

TITLE

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

ENTIRE AGREEMENT

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

Chapter 12

Cancellation

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

Index