enCap User Guide

EDM04-09

Protection Against Harmful Interference

When present on equipment this manual pertains to, the statement "This device complies with part 15 of the FCC rules" specifies the equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the Federal Communications Commission [FCC] Rules.

These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment.

This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications.

Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at their own expense.

Extra Components and Materials

The product that this manual pertains to may include extra components and materials that are not essential to its basic operation, but are necessary to ensure compliance to the product standards required by the United States Federal Communications Commission, and the European EMC Directive. Modification or removal of these components and/or materials, is liable to cause non compliance to these standards, and in doing so invalidate the user’s right to operate this equipment in a Class A industrial environment.

Disclaimer

Whilst every effort has been made to ensure accuracy, neither Endace Technology Limited nor any employee of the company, shall be liable on any ground whatsoever to any party in respect of decisions or actions they may make as a result of using this information.

Endace Technology Limited has taken great effort to verify the accuracy of this manual, but nothing herein should be construed as a warranty and Endace shall not be liable for technical or editorial errors or omissions contained herein.

In accordance with the Endace Technology Limited policy of continuing development, the information contained herein is subject to change without notice.

Published by:

Endace Technology® Ltd
Level 9
85 Alexandra Street

PO Box 19246
Hamilton 3244
New Zealand

Phone: +64 7 839 0540
Fax: +64 7 839 0543
support@endace.com
www.endace.com

International Locations

New Zealand
Endace Technology Limited
Building 7, Lambie Drive
PO Box 76802
Manukau City 2241
New Zealand

Phone: +64 9 262 7260
Fax: +64 9 262 7261

Americas
Endace USA® Ltd
Suite 220
11495 Sunset Hill Road
Reston, Virginia 20190
United States of America

Phone: +1 703 382 0155
Fax: +1 703 382 0155

Europe, Middle East & Africa
Endace Europe® Ltd
Sheraton House
Castle Park
Cambridge CB3 0AX
United Kingdom

Phone: +44 1223 370 176
Fax: +44 1223 370 040

Copyright 2006-2007 Endace Technology Ltd. All rights reserved.

Contents

Introduction

Overview

Packet capture is the basis for all network monitoring. However, currently the available industry standard pcap-based packet capture solutions are suitable only for lower speed networks. Their performance over Gigabit networks is usually poor by comparison.

enCap is a high speed packet capture library that turns a commodity PC into an efficient and economical network measurement device.

enCap enables you to create efficient applications such as traffic balancers or packet filters using just a few lines of code. This is because enCap is a pure userland library that is based on a special kernel driver.

It allows any developer who is able to program in C to write such applications without the need to learn the kernel insights.

Note: The accelerated enCap driver is currently available for Endace supplied Intel® Pro 1000 Server Adapter, (copper 10, 100, 1000 or 10Base-T, 100 Base-TX, 1000 Base-T) Ethernet cards only. To use enCap you must have one of these cards installed.

Features

enCap offers a new approach to packet capture based on the following:

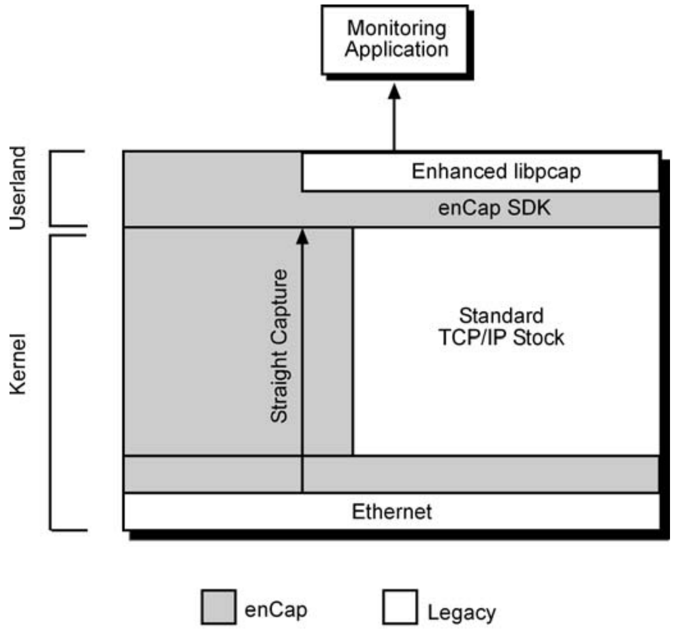
- Ability to capture packets at wire speed,
- No need for custom network cards or hardware platforms,
- Support for legacy pcap–based applications to allow them to work with enCap without code changes.

The main building blocks used by enCap are:

- An accelerated kernel driver that provides low-level support and Ethernet device programming,
- User space enCap SDK that can be used through an enhanced libpcap that provides transparent enCap support to legacy pcap-based applications.

Architecture

The diagram below illustrates the enCap architecture.



Installation

Introduction

The enCap installation CD contains binary packages suitable for a range of major GNU/Linux distributions. These include:

- Debian Sarge,
- RHEL v4,
- RHEL v3,
- SuSE v10.0

! If the install script does not successfully complete please refer to Installing the *Linux Kernel Module*, *Installing libencap* and *Installing Libpcap*. later in this chapter for more information.

If you experience problems with other applications after installing enCap please refer to *Distribution Specific Installations* later in this chapter for more information.

Installing the Card

Follow the steps below to install the Endace supplied network card in your PC:

- Turn power to the PC OFF,
- Remove the bus slot screw and cover,
- Using an approved ESD protection device attach the end with the strap to your wrist and pull or clip firmly so there is firm contact with your wrist,
- Securely attach the clip on the other end of the strap to a solid metal area on the PC chassis,
- Insert the network card into bus slot ensuring it is firmly seated ,
- Check the free end of the card fits securely into the card-end bracket that supports the weight of the card,
- Secure the card with the bus slot cover screw,
- Turn power to the computer ON.

Installing enCap

! Before beginning this installation ensure you are logged on to your machine as the `root user`. If you do not login as the root user you will not be able to complete the installation.

To install enCap perform the following steps:

- Insert the enCap installation CD into your CDROM drive.
- Run the following script: `./install.sh`
- Alternatively you can copy the contents of the CD to a local directory and run the install script from there. For example:

```
cp –R <mount path> ~/encap-cd
cd ~/encap-cd
./install.sh
```

- The install script will automatically detect your distribution type and install enCap on your machine using your native package management system.

Installing the enCap License

enCap requires a license key for each Ethernet card used. It is specific to the Endace supplied network card on which enCap is to be activated.

To install the enCap license perform the following steps:

- Enter the 32 character license key which can be found on the sleeve of the installation CD with your Serial Number and card MAC Address.

  Note: If you do not enter the correct license key you will continue being prompted until it is correct. You may abort this process using the CTRL +C key combination.
- Once you enter the license key it is copied into the `/etc/enCap.license` file.
- Once you have successfully entered your license key the message `enCap successfully installed` will display.

  Note: enCap license issues are reported in syslog.
- If you are using enCap with enhanced libpcap or installing enCap aware applications you do not need to complete any further installation steps and enCap is ready for use.

  Note: In this case you may skip the remainder of this chapter and go straight to the Usage chapter on page 9.
- If you are using third party libpcap applications, please refer to the appropriate documentation relating to these products for further information.

! Some pcap-based applications such as tcpdump may be statically linked against libpcap. These will need to be rebuilt against the new libpcap to benefit from the enCap enabled libpcap.

In the case of tcpdump under RHEL the enCap installation will replace the statically linked libpcap with a dynamically linked tcpdump.

Recompiling a Kernel Module

Introduction

The automated install script attempts to install a suitable kernel driver module. However there may be cases where it does not successfully complete. This may be because you have a newer version of the Linux kernel installed on your machine and therefore require a later kernel module, or enCap may not have recognized your Linux distribution.

In this case you need to compile your own kernel module from source. There are two methods of generating a kernel module. They are:

- Use your distribution packaging tools and then follow with either the *RPM* or *.deb* procedure listed below. These procedures will compile two packages for you to install. One is a kernel module package and the other is a common package containing initialisation scripts.
- Use the *SRC* procedure listed below to manually compile and install the kernel module. This is the most reliable method however it is independent of your Linux distribution native package management system.

Redhat Packages/RPM

- To build a new module for your existing kernel on a *RPM* based distribution, run the following command with superuser privileges:
  ```
  cd <mount path>/pkg/SRPMS
  rpmbuild --rebuild pkg/SRPMS/e1000encap-6.3.9-1.src.rpm
  ```
- When this successfully compiles, the new RPM will be stored in your distributions RPM directory. This directory varies between different distributions but looks similar to:
  ```
  /usr/src/[rpm|packages|redhat]/RPMS/<arch>/e1000encap-*7.0.33-1.<arch>.rpm
  ```
- You can then install the new kernel package using the commands:
  ```
  rpm –e –nodeps e1000encap
  cd <mount path>/pkg/<distro>
  rpm –U e1000encap-7.0.38-2.*.rpm
  ```

Debian Packages/.deb

- *Debian* based distributions provide a utility called *make-kpkg* which allows you to create kernel module packages from a *debian* kernel source package. You can install a *debian* kernel-source package for enCap from the root directory of the CD with the command:
  ```
  cd <mount path>/pkg/debian/bin
  dpkg -i e1000encap-source_7.0.38-3_all.deb
  apt-get install kernel-package
  cd /usr/src
  tar -jxvf e1000encap.tar.bz2
  cd <linux-kernel-source-directory>
  make prepare
  make-kpkg –-added-modules e1000encap modules
  ```
- The new kernel package will now be in the `/usr/src` directory, install it with
  ```
  dpkg -i e1000encap-modules-<kernel version>_7.0.38-3_i386.deb
  ```

Note: For further details on usage of *make-kpkg* please refer to the associated man page.

Compiling from Source Tarball

- The most common and reliable method for installing the kernel module is to compile the module from source using the following commands:
  ```
  cd <mount path>/pkg/tgz
  tar -zxvf e1000encap-7.0.38.src.tar.gz
  cd e1000encap-7.0.38
  make
  make install
  depmod e1000encap
  ```
- In order to start enCap automatically at boot time you must start the init scripts with the following commands:
  ```
  cd<cd mount path>/pkg/tgz
  tar –C/-zxvf e1000encap-common-7.0.38.tgz ./etc/init.d/encap
  ln -s /etc/init.d/encap/etc/rc5.d/S20encap/etc/init.d/encap start
  ```

Note: The location of the `rc5.d` directory varies between different distributions

Installing Libencap

- If you have installed the kernel module as a package, you can install the *libencap* and *libencap-devel* packages from the CD using your normal package tools.
- If you installed the e1000encap kernel module from source you will not be able to install the prebuilt *libencap* binary package because there will be a dependency failure. There are two ways to avoid this problem.
  1. You may ignore the dependency checking feature of your packaging system;
     On rpm based system use `rpm -U –nodeps <package>`
     On debian based systems use dpkg `-i –force-depends <package>`
  2. Alternatively you can install the tgz version of libencap using the command
     ```
     cd <mount path>/pkg/tgz
     tar –C / -zxf libencap1-1.tgz
     ```
- You can use the same method to install the *libencap-devel* package, which contains static libraries and headers.

Installing Libpcap

- *Libpcap* is provided in both source and binary format.
- The binary package depends on the *libencap* package being installed however you can use the binary tgz with the following command:

  ```
  cd <mount path>/pkg/tgz
  tar –C / -zxvf libpcap-encap-0.9.4.tgz
  ```

- You can also use the same method to install the *libpcap-encap-dev* package which contains files used to compile applications based on libpcap.

  Note: You do not need *libpcap-encap-dev* installed to run libpcap based applications.

- To build libpcap from source use the following commands:

  ```
  tar -zxvf libpcap-encap-0.9.4.src.tar.gz
  cd libpcap-encap-0.9.4
  ./configure
  make
  make install
  ```

Note: It is likely your distribution already provides a version of libpcap without the enCcap enhancements. This means if you install *libpcap-encap* from source you will have two versions of libpcap installed on your system.

You will need to ensure the applications you use to capture data are using the enCap version of libpcap.

Using Libpcap

Example Session

Because enCap is an enhancement to libpcap it is only possible to demonstrate its usage using other applications.

Tcpdump is a common application that uses libpcap and the example below shows a tcpdump session.

Note: To use enCap, the card on which it is activated must be dedicated to enCap. You can not use it as a normal network interface.

The following example assumes you have successfully installed the enCap software and you are logged in as the `root user`.

```
ls /dev/encap/
eth1
ifconfig eth1
eth1   Link encap:Ethernet  HWaddr 00:00:00:00:00:00
BROADCAST MULTICAST  MTU:1500  Metric:1
RX packets:0 errors:0 dropped:0 overruns:0
frame:0
TX packets:0 errors:0 dropped:0 overruns:0
carrier:0
collisions:0 txqueuelen:1000
RX bytes:0 (0.0 b)  TX bytes:0 (0.0 b)
Base address:0xac00 Memory:cffe0000-d0000000
tcpdump -D
1.eth0
2.any (Pseudo-device that captures on all interfaces)
3.lo
```

The card identifier will vary depending upon how many cards you have installed. In this case the card is configured as `eth1`.

Note: These two commands show that *eth1* has not been configured yet. `ifconfig` doesn't report the interface in the UP state and tcpdump doesn't recognize the interface as available.

```
$ ifconfig eth1 promisc up
$ ifconfig eth1
eth1   Link encap:Ethernet  HWaddr 00:07:E9:19:E6:60

UP BROADCAST  PROMISC MULTICAST  MTU:1500
Metric:1
RX packets:0 errors:0 dropped:0 overruns:0
frame:0
TX packets:0 errors:0 dropped:0 overruns:0
carrier:0
collisions:0 txqueuelen:1000
RX bytes:0 (0.0 b)  TX bytes:0 (0.0 b)
Base address:0xac00 Memory:cffe0000-d0000000
$ tcpdump  -D
1.eth0
2.eth1
3.any (Pseudo-device that captures on all interfaces)
4.lo
```

The interface has been brought up and placed in promiscuous mode. This allows you to capture network traffic destined for other host addresses and tcpdump recognizes it as being available.

Tells tcpdump which interface to listen to. In this case eth1.

Specifies how many to capture. In this case just 1.

```
   $ tcpdump -i eth1 -c 1 -n
   Successfully open /dev/encap/eth1
   tcpdump: WARNING: eth1: no IPv4 address assigned
```

Indicates enCap is correctly enabled.

The interface doesn’t need an IP address in order to capture data, so the warning can be safely ignored.

```
tcpdump: verbose output suppressed, use -v or -vv       for full protocol decode
   listening on eth1, link-type EN10MB (Ethernet),      capture size 96 bytes
   13:41:57.377457 arp who-has 192.168.1.1 tell   192.168.1.2
   1 packets captured
   1 packets received by filter
   0 packets dropped by kernel
```

You have just captured your first packet through enCap.

Note: If your license key is invalid enCap will fall back to the native libpcap capture method. This is shown in the following example.

```
$ tcpdump -i eth1 -c 1
Invalid encap license (eth1)
tcpdump: WARNING: eth1: no IPv4 address assigned
tcpdump: verbose output suppressed, use -v or -vv    for full protocol decode
listening on eth1, link-type EN10MB (Ethernet), capture size 96 bytes
13:41:57.377457 arp who-has 192.168.1.1 tell 192.168.1.2
1 packets captured
1 packets received by filter
0 packets dropped by kernel
```

Uninstalling

Overview

If for any reason you need to uninstall enCap you can do so by running the uninstall script included on the enCap Installation CD.

Note: Installing enCap does not install the uninstall script on your machine. You must run the script from the installation CD.

Uninstalling enCap does not prevent you from re-installing it again at some time in the future.

Running the Uninstall Script

Note: Before beginning this installation ensure you are logged onto you machine as `root user`. If you do not logon as root user you will not be able to complete the un-install.

- Insert the enCap installation CD into your CDROM drive
- Using your command line interface, run the script `./uninstall.sh` ensuring you are in the directory in which the CD is mounted.
- The `remove regular file/etc/encap_license` prompt allows you to chose whether to remove your enCap license or not. If you chose not to remove it, you will not have to re-enter the 32 character license key if you-install enCap in the future.

Re-installing Libcap

Once the uninstallation of enCap is complete you will be prompted to choose if you want to re-install the original *libpcap* that was on your machine before you installed enCap.

If you chose *No* you may have to manually re-install libpcap at a later date.

If you chose *Yes* it will automatically re-install either from the local cache or your machine or as a downloaded.

Updates

Overview

Updates to enCap will be notified to you using the contact email address you supplied on the enCap configuration form at the time you ordered enCap.

The notification will include advice of the available update(s) and a link to the Endace Customer Support website to enable you to download them.

Note: If the email address you originally supplied changes for any reason you should notify Endace Technical Support at support@endace.com to ensure you continue to receive enCap updates.

Troubleshooting

Overview

This section describes some common problems that you may experience with enCap and provides some possible solutions.

If you are still experiencing problems after using this section please contact Endace Customer Support at support@endace.com for further assistance.

Distribution Specific Installation

Introduction

Depending upon your Linux distribution you may encounter some problems during or subsequent to running the in stall script. Possible problems and suggested solutions are outlined below under each distribution.

SuSE

Only one driver should use the network card. It is possible that your distribution hardware detection will detect and install the e1000 driver rather than the e1000encap module which is required to use enCap.

Configure YAST to load the e1000encap Linux kernel module instead of e1000 as follows:

- From the top panel open the *Desktop* menu
- Start *YAST*
- In the left panel of YAST select '*network devices*'
- Click on 'Network Card'
- Select 'Intel PRO/1000 MT Server Adaptor'
- Press the *Edit* button to bring up the next screen
- Click the *Advanced* button and from the menu select '*Hardware Details*'
- Edit the box under '*Module Name*' from *e1000* to *e1000encap*

DEBIAN

If you have *libpcap0.8-dev* installed you need to remove it before you run the enCap install script `install.sh` . *libpcap0.8-dev* blocks the installation of the enCap enabled libpcap.

However you may install the *libpcap-encap-dev* package after the install completes, a prebuilt package is on the CD in the directory `pkg/debian/bin/`

RHEL/Fedora

During the first boot of the PC after plugging in the Endace supplied network card, the boot process will pause allowing you the opportunity to configure your network card.

When you see a blue/red screen labeled '*Kudzu Hardware Detection and Configuration*' screen press any key and a new screen will report that your network card has been added. You are then provided with three options. They are:

- `‘Configure’`
- `‘Cancel’`
- `‘Ignore’`

You should select `‘Ignore’` to allow your system to continue and compete the boot process.

Other Possible Problems

Problem	Action

Install fails with;
`bash: ./install.sh: /bin/bash: bad interpreter: Permission denied`
	`mount -o remount, exec <path-to-cd>`

Install fails with
`ls: /dev/encap/*: No such file or directory`
`WARNING: Could not detect encap enabled network card, i will not attempt to verify the product key`
	Ensure the network card is installed

enCap is falling back to pcap's default capture method.	Check the e1000encap kernel module is loaded and not the e1000,
tcpdump appears to hang when trying to capture data.	Use the `tcpdump -n` option to stop it trying to resolve addresses to names. It can not perform this function without transmitting.
The enCap network interface tries to automatically configure itself.	On rpm based distributions, disable the Network Manager system service.

Version History

Version	Date	Reason
1-2	April 2006	First releases
3	August 2006	Layout and formatting changes. General corrections.
4	October 2007	New template and general revision.