Libpcap and Third Party Applications

EDM04-21

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.

Website

http://www.endace.com

Copyright 2007 - 2011 Endace Technology Ltd. All Rights reserved

Contents

Introduction

This document describes the correct installation of Libpcap for use with third party applications and Endace DAG cards. These third party applications include protocol analyzers, network monitors, network intrusion detection systems and packet sniffers.

The third party applications covered in this document are:

- Snort
- Tcpdump
- Tcpreplay
- Wireshark (Ethereal) / Tshark
- CoralReef

Winpcap

This user guide does not cover Winpcap. For more information refer to the Winpcap website www.tcpdump.org/wpcap.html.

Libpcap

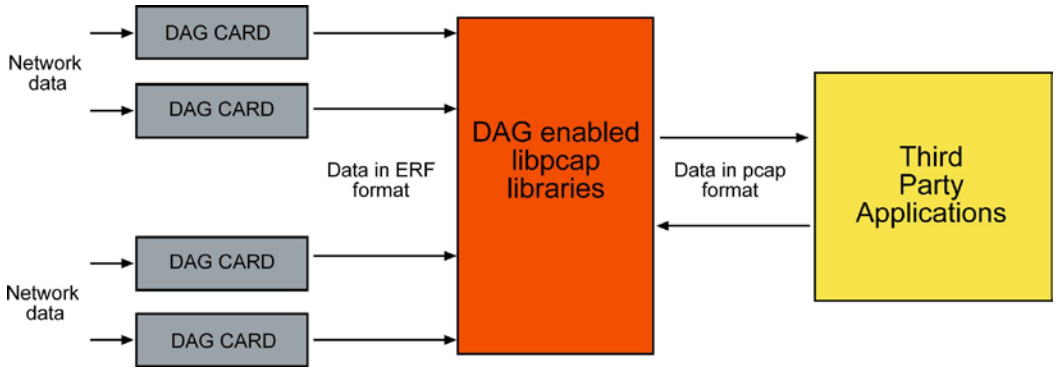
Libpcap is the implementation of pcap for Unix-like systems. Libpcap may be used by a program to capture packets travelling over a network. The Libpcap API is the packet capturing and filtering engine for many open source and commercial network tools.

Libpcap and DAG cards

Data packets from DAG cards are converted from native ERF format to pcap format using the Libpcap API.

In order to use some third party applications with Endace DAG cards you must use a DAG enabled version of Libpcap.

The following diagram shows the data transfer process:



DAG enabled libpcap library

To run the third party applications covered in this manual a DAG enabled version of Libpcap is needed.
Libpcap version 0.9.6 or greater is required.

This can be downloaded from our website:
www.endace.com/resources/tools/
or
www.tcpdump.org

Checking DAG software

The DAG software supplied with the DAG card must be installed on the computer for the third party applications to work with the DAG card.

For more information on installing DAG software refer to *EDM04-01 DAG Software Installation Guide*

Installing Libpcap

Note:
The third party application you want to use will determine whether you need to install the static or dynamic Libpcap libraries. For more information see *Applications covered in this document (page 5).*

The following procedures use "`libpcap-x.x.x.tar.gz`" to refer to the DAG enabled Libpcap version 0.9.6 or greater.

Install libpcap static library – default location

1. Unpack `libpcap-x.x.x.tar.gz`
2. Run the following commands:
   - `./configure --with-dag`
   - `make`
   - `make install`

   All of the Libpcap system files are in standard locations of `/usr/local/bin` and `/usr/local/lib`.

Install libpcap dynamic library – default location

1. Unpack `libpcap-x.x.x.tar.gz`
2. Run the following commands:
   - `./configure --with-dag`
   - `make shared`
   - `make install-shared`

   All of the Libpcap system files are in standard locations of `/usr/local/bin` and `/usr/local/lib`.
3. Create a link to the `libpcap.so.x.x.x` file from `libpcap.so` so the script recognizes the correct version of Libpcap using the following command:
   `ln –s libpcap.so.x.x.x libpcap.so`

Install libpcap static library – specified location

1. Unpack `libpcap-x.x.x.tar.gz`
2. Create a folder into which Libpcap will be installed.
   In the following example the `/root/pcap` folder is used.
3. Run the following commands:
   - `./configure --with-dag --prefix=/root/pcap`
   - `make`
   - `make install`

   All of the Libpcap system files are in the location of `/root/pcap`.

Install libpcap dynamic library – specified location

1. Unpack `libpcap-x.x.x.tar.gz`
2. Create a folder into which Libpcap will be installed.
   In the following example the `/root/pcap` folder is used.
3. Run the following commands:
   - `./configure --with-dag --prefix=/root/pcap`
   - `make shared`
   - `make install-shared`

   All of the Libpcap system files are in the location of `/root/pcap`.
4. Create a link to the `libpcap.so.x.x.x` file from `libpcap.so` so the script recognizes the right version of Libpcap using the following command
   `ln –s libpcap.so.x.x.x libpcap.so`

Third party applications

Once Libpcap is installed and setup you can choose an appropriate third party application and follow the instructions to configure and communicate with the installed DAG cards.

Some third party applications that use Libpcap include tcpdump, Wireshark(Ethereal), Snort, nTop, tcpreplay, ssldump, Nmap.

Applications covered in this document

Application	Usage	Library type
Wireshark	protocol analyzer	static or dynamic
SNORT	Intrusion detection system	dynamic
tcpdump	Capture / analyzer	static
tcpreplay	Reproduce and capture	Static
CoralReef	Capture / analyzer	Static or unused

Installing SNORT

Endace recommends SNORT to be used with dynamic Libpcap libraries.

Install the DAG enabled Libpcap into non-default folders. Installing into the default locations may cause problems with other versions of Libpcap.

For this example Libpcap has been installed into `/root/pcap`.

1. Go to the `root/pcap/lib` folder where the DAG enabled libpcap is installed.
2. If the `libpcap.a` file is present, delete it.
3. Unpack `snort-x.x.x.x.tar.gz`
4. Create a folder into which SNORT will be installed.

   In the following example the `/root/snort` folder is used.
5. Run the following commands, (each bullet point is a new line)
   - `./configure --prefix=/root/snort --with-libpcap-includes=/root/pcap/include --with-libpcap-libraries=/root/pcap/lib`
   - `make`
   - `make install`
6. Run the following code to make sure SNORT links the correct Libpcap version in the specified path before SNORT is executed.

   `export LD_LIBRARY_PATH=/root/pcap/lib:$LD_LIBRARY_PATH`
7. Run `ldd /root/snort/bin/snort`. The full path to `libpcap.so` is displayed.

   If `/root/pcap/lib/libpcap.so` is displayed the correct version of Libpcap is used.

Installing Tcpdump

Tcpdump uses statically linked Libpcap libraries.

Endace recommends Tcpdump to be configured with the DAG enabled Libpcap libraries installed in a non-default location.

1. Unpack `tcpdump-x.x.x.tar.gz`
2. Create a folder into which Tcpdump will be installed.
   In the following example the `/root/tcpdump` folder is used.
3. Run the following commands, (each bullet point is a new line)
   - `./configure --prefix=/root/tcpdump CPPFLAGS=-I/root/pcap/include/ LDFLAGS=-L/root/pcap/lib`
   - `make`
   - `make install`
4. Run the following code to check that tcpdump is linked with the appropriate version of Libpcap
   `/root/tcpdump –help`
   The version of Libpcap used by Tcpdump is displayed on screen.

Installing Tcpreplay

Tcpreplay uses statically linked Libpcap libraries.

Endace recommends Tcpreplay to be configured with the DAG enabled Libpcap libraries installed in the **default** location.

1. Unpack `tcpreplay-x.x.x.tar.gz`
2. Create a folder into which Tcpreplay will be installed.
   In the following example the `/root/tcpreplay` folder is used.
3. Run the following commands:
   - `./configure –-prefix=/root/tcpreplay`
     After `./configure` has run the version of Libpcap used is displayed on screen.
   - `make`
   - `make test`
   - `make install`

   Tcpreplay is now installed into `/root/tcpreplay`

Installing Wireshark / Tshark

Wireshark for Windows

Wireshark is a GUI based program, installed using an installation wizard. Winpcap libraries are installed as part of the Wireshark installation.

Wireshark / Tshark for Linux systems

Tshark is the console version of Wireshark and is designed to be run on the command line. Tshark is installed as part of the Wireshark package.

Tshark uses statically linked Libpcap libraries.

Tshark has many dependencies that it needs to compile properly. These dependencies are various libraries that have to be installed in default locations for Tshark to link to them.

Endace recommends Tshark to be configured with the DAG enabled Libpcap libraries installed in the **default** location.

1. Unpack `wireshark-x.x.x.tar.gz`.
2. Run the following commands to compile Tshark:
   - `./configure`
   - `make`
   - `make install`

   If Tshark does not compile properly there will be libraries missing. After compiling has failed the libraries needed are listed on screen.
   - `Download and install the missing libraries using the following commands: apt-get install libgtk2.0-dev libpango1.0-dev libcairo2-dev libx11-dev libxext-dev libxinerama-dev libxi-dev libxrandr-dev libxcursor-dev libxfixes-dev libxdmcp-dev libxft-dev`
   - Recompile using step 2.
3. Run the following command to check that Tshark can communicate with the installed DAG card(s):
   - `tshark –D`

   The following is displayed on screen:

   ```
   1. dag0
   2. dag0:0
   3. eth1
   4. any (Pseudo-device that captures on all interfaces)
   5. lo
   ```

Installing CoralReef

Installing CoralReef without libpcap

This method of installation links CoralReef to the DAG libraries. This method allows CoralReef to access full ERF metadata and high resolution timestamps.

CoralReef can read data from DAG cards and DAG files natively using the DAG API via libdag.

1. Unpack `coral-x.x.x.tar.gz`
2. Run the following commands:
   - `./configure –-with-dag =/usr/local/`
   - `make`
   - `make install`

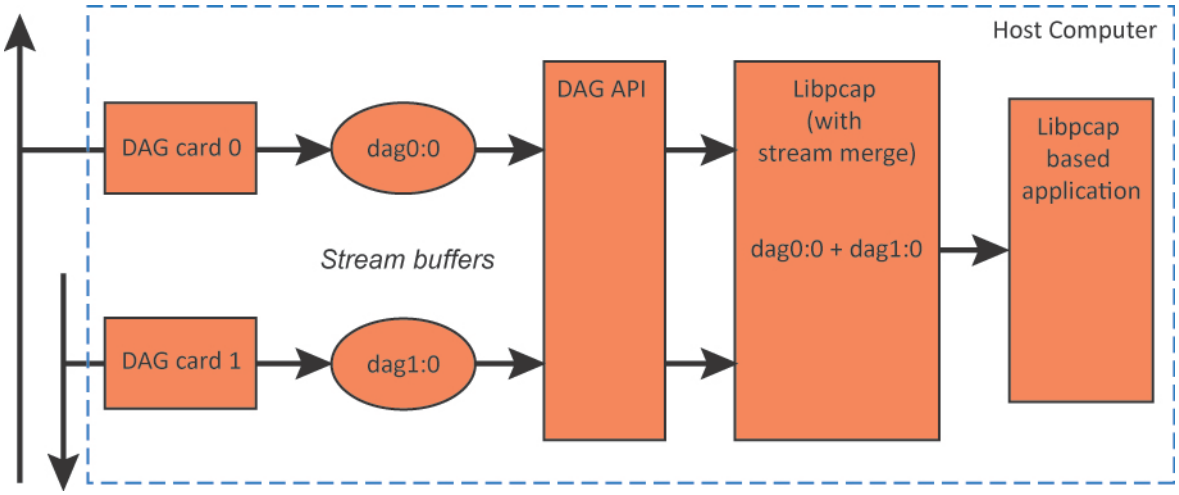
   CoralReef is now installed.

Example : usage for DAG 4.5G2 (dag2)

```
/crl_rate /dev/dag2 –C"iomode=proto=Ethernet,nif=2,first=110,varlen"
```


Merging captured streams

Libpcap allows you to merge **two** captured streams together (in the correct time order). This merged stream can then be used by any libpcap based application. This feature is applicable to DAG devices only.



Requirements

The two DAG card clocks must be synchronized to ensure the time ordering of the two streams is accurate. See the appropriate DAG Card User Guide for details.

Stream device name

Libpcap sees each stream buffer as a virtual device and identifies it by a stream device name, for example:

```
dagx:y
```

Where:

- `x` is the name of the card, and
- `y` is the number of the stream.

Types of merging

There are two types of merging available:

- **Standard merging**, the time order of the packets is *not* preserved.
  This option uses the - operator.
- **Ordered merging**, the time order of the packets is preserved. This is CPU intensive.
  This option uses the + operator.

Merging streams

To merge two streams together, run the libpcap application with the traffic input set as the two stream device names separated by the required operator, as defined above.

For example, to merge the following streams:

- DAG card 0, stream 0
- DAG card 1, stream 2

into one, time ordered stream to be used by TCPDump, type the following:

```
tcpdump -i dag0:0+dag1:2
```

Version History

Version	Date	Reason
1	December 2007	First release.
2	February 2008	Added CoralReef section.
3	August 2009	Updated for DAG software release 3.4.1. Updated front matter. Added Merging Captured Streams.
4	April 2010	Imported into AuthorIT. Rebranded. Corrected Merging captured streams operator.
5	March 2011	Corrected static and dynamic library installation commands.

endace.com