dagfwddemo Program User Manual

EDM04.05-04r1

Endace Measurement Systems | New Zealand | www.endace.com

Leading Network Intelligence

Published by:

Endace Measurement Systems® Ltd
Building 7
17 Lambie Drive
PO Box 76802
Manukau City 1702
New Zealand
Phone: +64 9 262 7260
Fax: +64 9 262 7261
support@endace.com
www.endace.com

International Locations

New Zealand

Endace Technology® Ltd
Level 9
85 Alexandra Street
PO Box 19246
Hamilton 2001
New Zealand
Phone: +64 7 839 0540
Fax: +64 7 839 0543
support@endace.com
www.endace.com

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
support@endace.com
www.endace.com

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
support@endace.com
www.endace.com

Typographical Conventions Used in this Document

- Command-line examples suitable for entering at command prompts are displayed in `mono-space courier font`. The font is also used to describe config file data used as examples within a sentence. An example can be in more than one sentence.

  Results generated by example command-lines are also displayed in `mono-space courier font.`

- The software version references such as 2.3.x, 2.4.x, 2.5.x are specific to Endace Measurement Systems and relate to Company software products only.

Protection Against Harmful Interference

When present on product this manual pertains to and indicated by product labelling, 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 his 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.

Table of Contents

1.0 PREFACE

1.1 User Manual Purpose

Description

The purpose of the User Manual is to identify and explain:

- The Endace `dagfwddemo` program for Endace DAG 3.7G and DAG 4.3GE cards

1.2 Prerequisites for `dagfwddemo` Program

Description

The pre-requisites for the `dagfwddemo` program is:

- Endace DAG 3.7G and DAG 4.3GE network monitoring cards
- Latest version of `libpcap` installed, version 0.8.3 or higher because `dagfwddemo` uses `libpcap` to perform BPF filtering.

The latest version of `libpcap` can be downloaded from the Endace website http://www.endace.com/libpcap.htm, or winpcap for the Windows operating system.

1.3 References

Description

The following are source references for this document:

1. Steven McCanne and Van Jacobson. *The BSD Packet Filter: A New Architecture for User-level Packet Capture.* In Proceedings of Winter 1993 USENIX Conference, pages 259 – 269. USENIX Association, January 1993. Available online: http://citeseer.ist.psu.edu/mccanne92bsd.html

2. The Tcpdump website. [Online]. http://www.tcpdump.org/

2.0 APPLYING DAGFWDDEMO FILTER

Introduction

The Endace DAG 3.7G and DAG 4.3GE cards have the ability to receive and transmit packets directly from a single memory buffer. This enables cards to forward packets from one interface to the other without copying them, sometimes referred to as zero-copy mode of operation.

The `dagfwddemo` is a program that applies a filter to traffic forwarded by a DAG 3.7G and DAG 4.3GE card. The filter is an arbitrary BSD Packet Filter (BPF) expression specified on the command line.

Within the architecture packets received on interface 0 will be transmitted on interface 1 and vice versa.

Figure

Figure 1-1 shows the `dagfwddemo` program architecture.

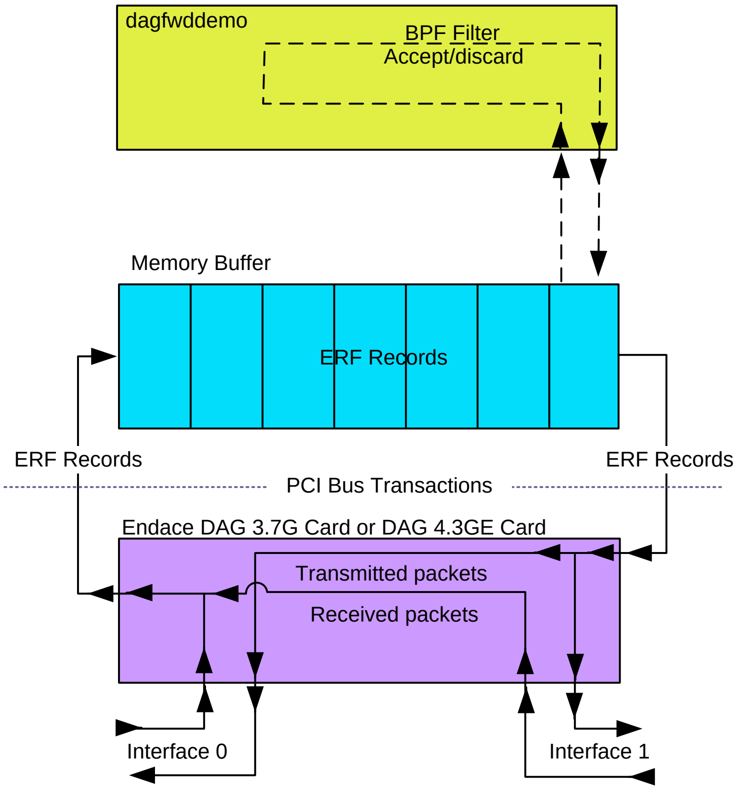

Figure 1-1. The `dagfwddemo` Program Architecture.

In this chapter

This chapter covers the following sections of information.

- Configure DAG 3.7G Card
- Configure DAG 4.3GE Card
- Command-line Arguments
- Traffic Statistics Sample Output
- dagfwddemo Program Examples

2.1 Configure DAG 3.7G Card

Description Configuring the DAG 3.7G card involves loading the DAG driver and configuring the card. The operation mode is restored after using the `dagfwddemo` program.

Procedure Follow these steps to configure the DAG 3.7G card.

Step 1. Load DAG Driver

Load the card DAG driver and firmware as described in the DAG 3.7G Card User Manual.

Step 2. Configure Card

Configure the card for inline operation using the `dagthree` command:

```
dagthree –d dag0 default overlap
```

NOTE: The optional argument `ifaceswap` can be used to have the card's hardware perform port forwarding.

The `ifaceswap` argument should be used in conjunction with the `–i` option in `dagfwddemo`. This ensures the port number is changed only once.

Step 3. Restore Operation Mode

After use, restore the standard mode of operation using the `dagthree` command before resuming standard packet capture or transmission:

```
dagthree –d dag0 default rxtx
```

NOTE: If the optional argument `ifaceswap` has been used to configure the card, the `noifaceswap` argument is used to restore the operation mode.

2.2 Configure DAG 4.3GE Card

Description

Configuring the DAG 4.3GE card involves loading the DAG driver, configuring the card. After use of the `dagfwddemo` program, the operation mode is restored using the `dagfour` command.

Procedure

Follow these steps to configure the DAG 4.3GE card.

Step 1. Load DAG Driver

Load the card DAG driver and firmware as described in the DAG 4.3GE Card User Manual.

Step 2. Configure Card

Configure the card for inline operation using the `dagfour` command:

```
dagfour –d dag0 default overlap
```

Step 3. Restore Operation Mode

After use, restore the standard mode of operation using the `dagfour` command before resuming standard packet capture or transmission:

```
dagfour –d dag0 default rxtx
```

2.3 Command-line Arguments

Description

By default, the `dagfwddemo` will change the interface number of received packets so that they can be forwarded on the other interface.

The general form of a `dagfwddemo` command, with BPF expression being contained in double quotes (“ “) is:

```
dagfwddemo [options] "bpf expression"
```

The command-line arguments and options recognised by `dagfwddemo` are presented here in a short form followed by the long form equivalent.

`-d`

`--device` Followed by the device name of the DAG card to configure, for example `dag0`

If the **–d** flag is not present then the default DAG card is assumed to be `dag0`

`-h`

Continued on next page

2.3 Command-line Arguments, continued

Description, continued

`-i`

Description output from **`–h`**: ‘do not change the port interface number’.

When using the 3.7G card if port forwarding is occurring in the firmware, the **`-i`** option is used to stop the interface number being changed by the software.

`-t<seconds>`

Runtime in seconds, default is run forever.

`-R`

Low latency receive mode.

Can also be used with **`–T.`**

This option will receive data as soon as possible, reducing the latency of receiving packets. This may cause slower throughput and more cpu usage when a lot of data is being received.

`-T`

Low latency transmit mode.

Can also be used with **`-R`**

This option will transmit data as soon as it is available, reducing latency. This may cause slower throughput and more cpu usage when a lot of data is available to transmit.

`?`

`--help`

If this flag is present then the `dagfwddemo` displays a help message and then exits.

`-V`

`--version`

Display version information for the `dagfwddemo`

2.4 Traffic Statistics Sample Output

Description

When `dagfwddemo` begins it displays the receive (stream 0) and transmit (stream 1) poll parameters. While running it prints three lines of traffic statistics to the screen each second, as shown below.

```
# dagfwddemo –d dag0 ""
 stream  0,  mindata:   16,  maxwait:   0.0,     poll:   0.0
 stream  1,  mindata:   16,  maxwait:   0.0,     poll:   0.0

               Interface 0        Interface 1       Total
 Received      1267      1267     1943     1943     3210     3210
 Dropped          0         0        0        0        0        0
 Rejected         0         0        0        0        0        0
 Received      1001      2268     1286     3229     2287     5497
 Dropped          0         0        0        0        0        0
 Rejected         0         0        0        0        0        0
 Received       969      3237     1329     4558     2298     7795
 Dropped          0         0        0        0        0        0
 Rejected         0         0        0        0        0        0
 Received      1273      4510     1440     5998     2713    10508
 Dropped          0         0        0        0        0        0
 Rejected         0         0        0        0        0        0
```

Line Terms

The line terms are described in the following table.

Term	Description
Received.	The received line displays the number of packets received on each interface, in the following order: • Packets received on interface 0 in the last second • Total packets received on interface 0 • Packets received on interface 1 in the last second • Total packets received on interface 1 • Total packets received in the last second on both interfaces • Total packets received on both interfaces

Continued on next page

2.4 Traffic Statistics Sample Output, continued

Line Terms, continued

Term	Description
Dropped.	The dropped line displays the number of packets that were dropped because they were invalid, such as the RX error bit was set in the ERF header, in the following order: • Packets dropped on interface 0 in the last second • Total packets dropped on interface 0 • Packets dropped on interface 1 in the last second • Total packets dropped on interface 1 • Total packets dropped in the last second on both interfaces • Total packets dropped on both interfaces
Rejected.	The rejected line displays the number of packets that were rejected by the BPF filter expression in the following order: • Packets rejected on interface 0 in the last second • Total packets rejected on interface 0 • Packets rejected on interface 1 in the last second • Total packets rejected on interface 1 • Total packets rejected in the last second on both interfaces • Total packets rejected on both interfaces

2.5 `dagfwddemo` Program Examples

Introduction

The examples of the `dagfwddemo` program include the Pass ICMP Packets, Pass TCP and ICMP Packets, and Pass TCP Packets by Host and Port.

In this section

This section covers the following topics of information.

- Pass ICMP Packets
- Pass TCP and ICMP Packets
- Pass TCP Packets by Host and Port

2.5.1 Pass ICMP Packets

Description The following filter expression will allow ICMP packets to pass between the two interfaces:

```
dagfwddemo –d dag0 "icmp"
```

2.5.2 Pass TCP and ICMP Packets

Description The following filter expression will allow only TCP and ICMP packets to pass between the two interfaces:

```
dagfwddemo –d dag0 "icmp and tcp"
```

2.5.3 Pass TCP Packets by Host and Port

Description The following filter expression will allow only TCP packets on port 80 (HTTP) with the host 'www.example.com' as source or destination to pass between the two interfaces.

```
dagfwddemo –d dag0 "tcp and host www.example.com and
port 80"
```