endace

accelerated

dagfwddemo User Guide

EDM04-04

www.endace.com

Published by:

Endace Limited

Building 7

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

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

Disclaimer

Whilst every effort has been made to ensure accuracy, neither Endace 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 Limited has taken great effort to verify the accuracy of this manual, but assumes no responsibility for any technical inaccuracies or typographical errors.

In accordance with the Endace Limited policy of continuing development, design and specifications are subject to change without notice.

Table of Contents

Chapter 1: Introduction

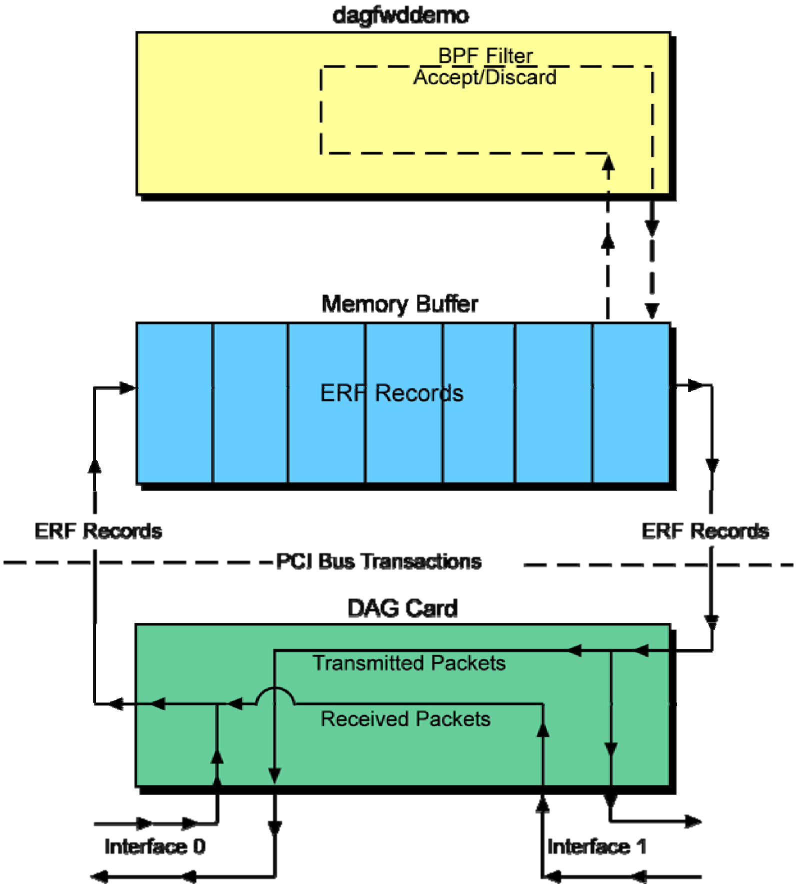
Overview

Some Endace DAG cards are able to receive and transmit packets directly from a single memory buffer. This allows you to forward packets from one interface to the other without the requirement to copy them. This mode of operation is sometimes referred to as “zero copy” mode.

`dagfwddemo` is an Endace supplied tool that demonstrates how you can apply a filter to the traffic forwarded by the DAG card. The filter is a BSD Packet Filter (BPF) expression specified in the command line.

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

The `dagfwddemo` architecture is shown below:



Note: `dagfwddemo` drops packets received with layer 2 errors, e.g. Ethernet TCS failures. All packets are bridged between interfaces at layer 2, IP TTL is not decremented. The DAG Card does respond to ARP, see user guide. While forwarding the card cannot be used for normal packet capture / transmission.

Supported DAG Cards

`dagfwddemo` is supported on all DAG cards which have a transmit option:

> **Note:** Whilst a DAG Card may support transmit the appropriate firmware must be installed to use `dagfwddemo`.

Prerequisites

To use `dagfwddemo` you must have the following installed on the PC from which you intend to run the program:

- One of the DAG cards which supports `dagfwddemo`.
- Version 0.8.3 or higher of libpcap.

> **Note:** `dagfwddemo` uses libpcap to perform BPF filtering which is available from the support section of the Endace website at www.endace.com

References

- For further information on BPF expressions please refer to the tcpdump website at http://www.tcpdump.org.
- The following is a source reference for this document:

  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.

  Also available online at: http://citeseer.ist.psu.edu/mccanne92bsd.html

Chapter 2: Configuring the Card

Standard Configuration

To configuring a DAG card for data capture do the following:

- Load the DAG device driver
- Load the images and program the FPGAs
- Set the link
- Check the link
- Configuring the connections

This process is detailed in the *Installation* and *Configuring the Card* chapters of the appropriate Card User Guide for the DAG card you are configuring.

> **Note:** The DAG Card User Guides are included on the CD shipped with the DAG card and are also available from the support section of the Endace website at www.enadce.com

Inline Configuration

To use `dagfwddemo` you must configure the DAG card for inline operation.

- For DAG 3.7G and DAG 3.8S cards use:
  ```
  dagthree –d0 default overlap
  ```
- For the DAG 4.3GE card use:
  ```
  dagfour –d0 default overlap
  ```
- For all other DAG cards use:
  ```
  dagconfig –d0 default overlap
  ```

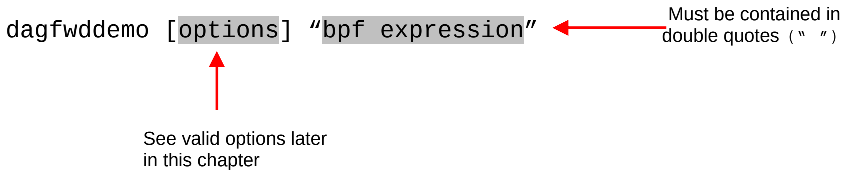
Restore Normal Configuration

When you have finished using `dagfwddemo` you must restore the card to normal operation to allow you to resume standard packet capture or transmission.

- For DAG 3.7G and DAG 3.8S cards use:
  ```
  dagthree –d0 default rxtx
  ```
- For the DAG 4.3GE card use:
  ```
  dagfour –d0 default rxtx
  ```
- For all other DAG cards use:
  ```
  dagconfig –d0 default rxtx
  ```

Commands

The form of a `dagfwddemo` command with BPF expression is:



```
dagfwddemo [options] “bpf expression”
```

Must be contained in double quotes (“ ”)

See valid options later in this chapter

`dagfwddemo` allows packets matching the user defined BPF filter to pass interface 0 and interface 1 bi-directionally. Any packets that do not match the filter are dropped. Specifying an empty filter i.e. `“”` allows all packets to be forwarded.

Example Expressions

The example BPF expressions described below are available in `dagfwddemo`.

Pass ICMP Packets

The following BPF expression will allow only ICMP packets to pass between the two interfaces:

```
dagfwddemo –d0 “icmp”
```

Pass TCP and ICMP Packets

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

```
dagfwddemo –d0 “tcp and icmp”
```

Pass TCP Packets by Host and Port

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

```
dagfwddemo –d0 “tcp and host www.example.com and port 80”
```

Don’t Pass TCP Packets by Port

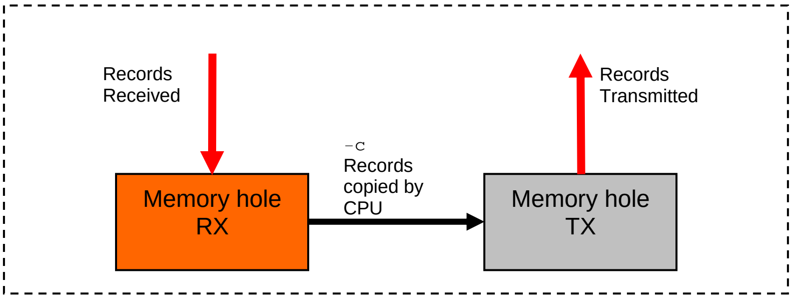
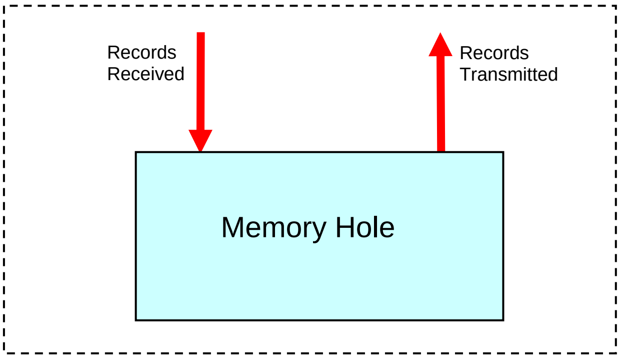
The following BPF expression will forward all traffic except port 80 TCP traffic.

```
dagfwddemo –d0 “not tcp port 80”
```

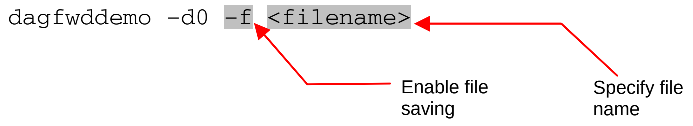
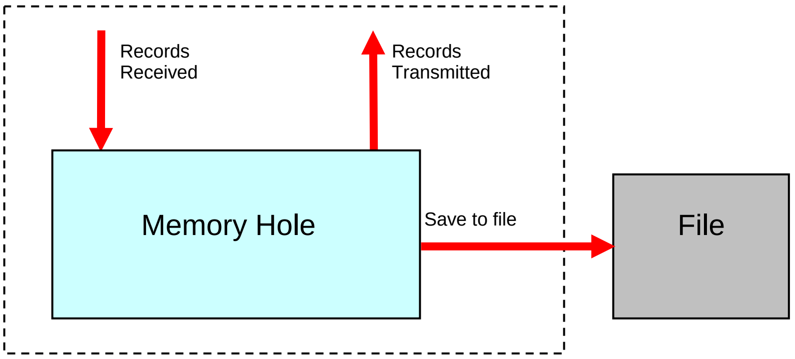
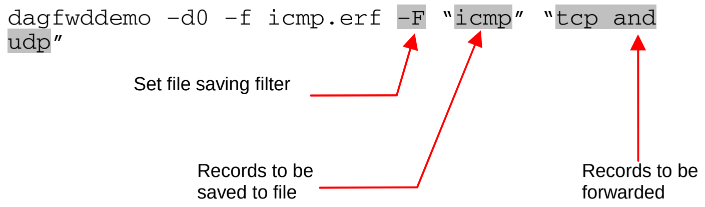
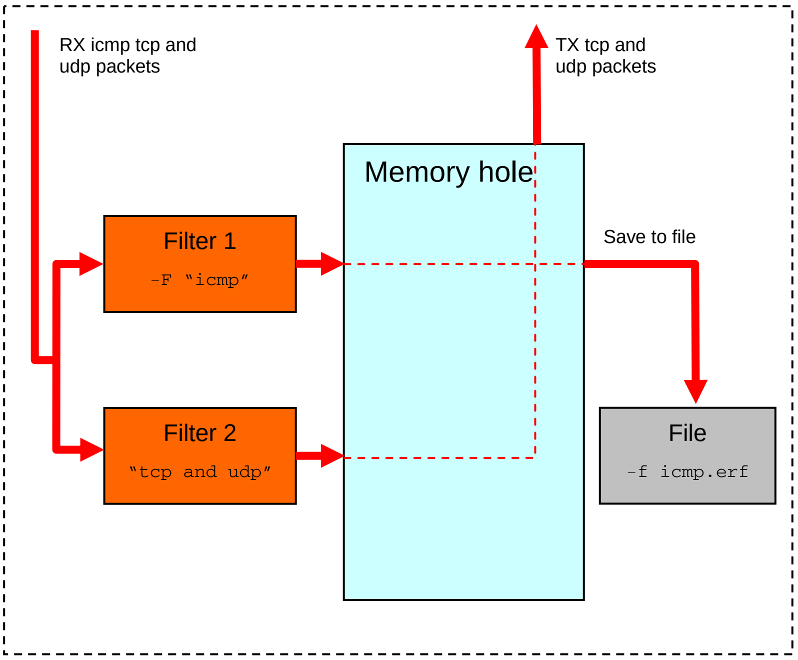
Valid Options

Option	Description
`-d`	The device identifier of the DAG card ie: `-d0` `dagfwddemo -d0` Select DAG card **Note:** If the `-d` option is not present in the command line, the default DAG card is assumed to be `-d0`.

`-h`
`-?`
`--help`
`--usage`
	Displays a help message and then exits
	- `-h` Displays help information:
	`dagfwddemo -d0 -h` Show help message

`-V` `--version`	Displays `dagfwddemo` version information `dagfwddemo -d0 -V` Show version information
`-c`	Copies records from one memory hole to another for transmitting. This works on normal memory hole setup. `dagfwddemo -d0 -c` Enable file copying Normal Memory Hole Setup  Records Received Records Transmitted -c Records copied by CPU Memory hole RX Memory hole TX Overlapped Memory Hole Setup 

Valid Options (Cont)

Option	Description
`-f`	Saves records to a specified file while forwarding those <u>same</u> records.  `dagfwddemo -d0 -f <filename>`  Records Received Records Transmitted Memory Hole Save to file File
`-F`	Define the filter used to select recorded packets.  `dagfwddemo -d0 -f icmp.erf -F “icmp” “tcp and udp”` Set file saving filter Records to be saved to file Records to be forwarded  RX icmp tcp and udp packets TX tcp and udp packets Memory hole Filter 1 -F “icmp” Filter 2 “tcp and udp” Save to file File -f icmp.erf **Note:** You must use the `-F` option with the `-f` option. This is independent of the packet forwarding filter. If `-F` is not used `“tcp and udp”` will be the filter used for records saved to file.

Valid Options (Cont)

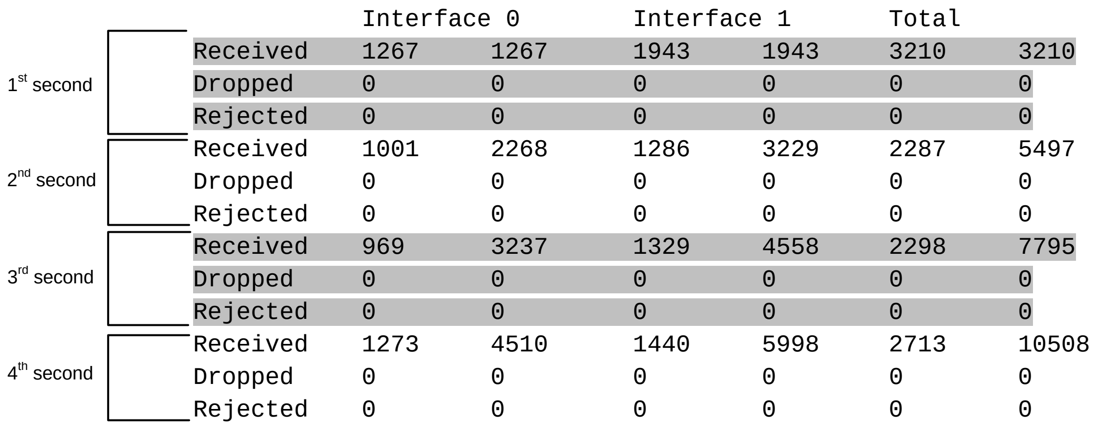
Option	Description
`-t`	Sets how long you want `dagfwddemo` to run. Time is specified in seconds. If no runtime is specified the default is *'run for ever'* `dagfwddemo -d0 -t <seconds>` Enable run time Actual time in seconds
`-R`	This forwards packets ASAP and sets low latency mode using 100% of CPU. `dagfwddemo -d0 -R` Enable Low latency receive mode **Note:** If `-R` mode is enabled `-B` is disabled.
`-m`	Minimizes the risk of lost records in the file by varying the size of the buffer to accommodate line rate. 256MB is the default buffer size. You must use the `-m` option with the `-f` option • `-m` Set the disk buffer size: `dagfwddemo -d0 -f <filename> -m <size in MB>` Enable the buffer size to be set Actual size of buffer in Mega Bytes
`-B`	Decreases the amount of CPU time required by buffering packets before they are transmitted. This is achieved by setting the maximum number of kilo bytes accumulated before transmission. `dagfwddemo -d0 -B <Size in kBs>` Enable bytes to be accumulated Actual size in kB
`-i`	DO NOT change the interface number when forwarding. You must use this option if you wish to retransmit packets on the port you receive on. `dagfwddemo -d0 -i` Enable DO NOT change interface number Note: The DAG 3.7G firmware automatically maps the interface number if `-i` is not enabled.

Example Output

When `dagfwddemo` begins it displays the receive (stream 0) and transmit (stream1) poll parameters.

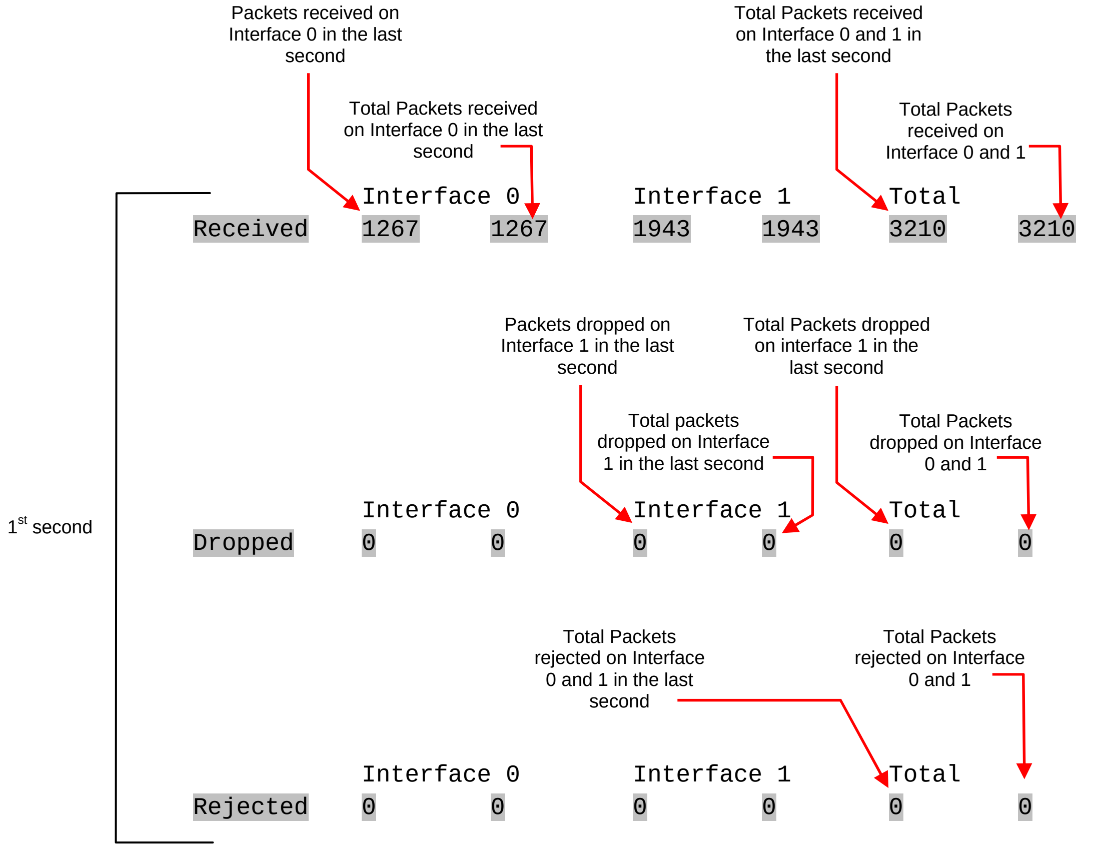
When running it prints three lines of traffic statistics to the screen every second as shown below:

```
# dagfwddemo –d0 “”
 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
```

1st second
2nd second
3rd second
4th second



```
            Interface 0         Interface 1         Total
Received    1267      1267      1943      1943      3210      3210

            Interface 0         Interface 1         Total
Dropped     0         0         0         0         0         0

            Interface 0         Interface 1         Total
Rejected    0         0         0         0         0         0
```

Packets received on Interface 0 in the last second
Total Packets received on Interface 0 in the last second
Total Packets received on Interface 0 and 1 in the last second
Total Packets received on Interface 0 and 1
Packets dropped on Interface 1 in the last second
Total packets dropped on Interface 1 in the last second
Total Packets dropped on interface 1 in the last second
Total Packets dropped on Interface 0 and 1
Total Packets rejected on Interface 0 and 1 in the last second
Total Packets rejected on Interface 0 and 1
1st second

Chapter 3: Troubleshooting

Reporting Problems

If you have problems with a DAG card or Endace supplied software which you are unable to resolve, please contact Endace Customer Support at support@endace.com.

Supplying as much information as possible enables Endace Customer Support to be more effective in their response to you. The exact information available to you for troubleshooting and analysis may be limited by nature of the problem. However the following items will assist a quick resolution:

- DAG card[s] model and serial number.
- Host PC type and configuration.
- Host PC operating system version
- DAG software version package in use
- Any compiler errors or warnings when building DAG driver or tools
- For Linux and FreeBSD, messages generated when DAG device driver is loaded. These can be collected from command `dmesg`, or from log file `/var/log/syslog`.
- Output of daginf
- Firmware versions from `dagrom –x`.
- Physical layer status reported by: `dagthree, dagfour, dagconfig`
- Network link statistics reported by: `dagthee –si, dagfour –si, dagconfig –si`
- Network link configuration from the router where available.
- Contents of any scripts in use.
- Complete output of session where error occurred including any error messages from DAG tools. The `typescript` Unix utility may be useful for recording this information.
- A small section of captured packet trace illustrating the problem.

Version History

The version history for this user guide is shown below

Version	Date	Reason
1-2	Pre 2006	Old Versions
3	August 2006	Added version history Added new options Added tables, descriptions and examples General revision and expansion of content