endace
accelerated

# Co-Processor IP filter Software Guide

EDM02-02

### 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 2005 - 2008 Endace Technology Ltd. All rights reserved.

# Contents



 

## IP filter software

The IP filter software allows you to load filter rule sets into the Co-Processor component of DAG cards. This enables you to filter, classify and steer packets based on user defined criteria.

The IP Filter software enables IP packets to be filtered based on:

- Ingress interface
- Protocol [IP, ICMP, IGRP, TCP, UDP]
- Source and destination IP address
- TCP and UDP source and destination port number
- TCP flags

The IP filter software includes:

- Xilinx images for the DAG 3.8S, DAG 4.3S and DAG 4.3GE cards and Co-Processor.
- Support for SC256 and SC128 Co-Processors.
- Snort Rule Compiler application for turning Snort-like rules into filters.
- Tcpdump Rule Compiler application for turning tcpdump-like rules into filters.
- Filter Loader application for loading filters onto the Co-Processor.

The DAG 3.8S, 4.3S and 4.3GE cards enable you to steer packets into two separate receive streams. This allows separate applications to operate on each receive stream.

### Conventions Used in this Document

- Command-line examples suitable for entering at command prompts are displayed in `mono-space courier font.`
- Results generated by example command-lines are also displayed in `mono-space courier font.`
- Information relating to functions not implemented in this beta version of this product are underlined

## Requirements

The requirements for installing the IP Filter software are:

- A DAG 3.8, 4.3S or 4.3GE card with an Endace Co-Processor fitted.
- DAG software (3.3.1 or greater).
  Customers with a current support contract can download this from the secure Endace website: https://www.endace.com/support.
  Refer to *EDM04-01 DAG Software Installation Guide* for details on how to install and compile the DAG software.

## Data capture

The following applications can capture data from DAG cards:

- DAG API
- Libpcap
  `libpcap` (0.9.7 or higher). You can download a copy from the following location:
  - http://www.tcpdump.org

**Note:** The DAG card and Co-Processor configuration feedback provided by a local system may vary from that shown in the following steps.

When changing the filter rule sets on the Co-Processor there is a delay before the new filters take effect. Changing a filter rule set is made of two parts:

- first load the filters rule sets to the DAG card - a process which is dependent on the number of filters loaded.
- swapping between the filter rule sets - this process occurs at the beginning of the next packet.

The above two operation are automatically completed by the `filter_loader` application. For further information see *EDM04-28 filter_loader Software Guide*.

For example, when receiving at 450MB per second, the time to load an 8K filter set and swap is under 0.5 of a second.

Please note there are different Co-Processor firmware images for the SC128 and SC256 Co-Processors.

**Note:** The SC128 Co-Processor capture packets without setup. The SC256 Co-Processor requires a filter rule set to be loaded before packets can be captured.

## How to tell what Co-Processor you have

Each Co-Processors has a different output from `daginf`.

### SC128 Co-Processor

```
Daginf
```

Output

```
id       0
model    DAG 3.8S
device   0x3800
phy addr 369098752
buf size 134217728 (128MB)
iom size 65536 (64kB)
copro    SC128
```

### SC256 Co-Processor

```
daginf
```

Output

```
id       0
model    DAG 4.3S
device   0x4300
phy addr 780140544
buf size 134217728 (128MB)
iom size 65536 (64kB)
copro    SC256 Rev C
```

## Configure DAG 3.8S Card and Co-Processor

To configure the DAG 3.8S card and Co-Processor, complete the following steps:

**Note:** The DAG 3.8S supports the SC128 Co-Processor only.

Load IP Filter firmware image for the DAG card by typing:

```
dagrom -d dag0 -rpy -f dag38s-ipf.bit
```

**Output**

```
current:edag38spci_cp1-ipf_v2_2 2v1000fg456 2005/08/18 12:24:05 *
stable:  edag38spci_erf_v2_13 2v1000fg456 2005/04/21 16:18:14
Card Serial: 3351
```

1. Load the IP Filter firmware images for the Co-Processor by typing:

   ```
   dagld -d0 -x dag38pp-terf.bit: copro-ipf38s.bit
   ```

   **Output**

   ```
   Waiting for Xilinx1 (dag38spp_erf_v2_8 2s300eft256) to program...
   FPGA Initialized.
   Starting to program
   ................................................
   File loaded.
   Done.
   Waiting for Xilinx2 (ec10gcp_ipf_v2_2 2v2000ff896) to program...
   FPGA Initialized.
   Starting to program
   ................................................
   File loaded.
   Done.
   ```

2. Configure DAG card.

   Type the following for an initial configuration for OC-12c operation:

   ```
   dagthree –d0 default oc12 slen=1540
   ```

   **Output**

   ```
   linkA   PoS noreset OC12c nolt0 fcl noeql enablea
   linkB   PoS noreset OC12c nolt0 fcl noeql enableb
   sonetA  noscramble slave
   sonetB  noscramble slave
   posA    nocrc pscramble
   posB    nocrc pscramble
   packet  varlen slen=1540 align64
   packetA drop=0
   packetB drop=0
   ipf     nodrop steer=stream0
   pcix    66MHz 64-bit buf=128MiB rxstreams=2 txstreams=0 mem=64:0:64:0
   ```

## Configure DAG 4.3GE Card and Co-Processor

To configure the DAG 4.3GE card and Co-Processor, complete the following steps:

**Note:** The DAG 4.3GE has different Co-Processor firmware images for the SC128 and SC256 Co-Processors.

1. Load the IP Filter firmware image for the DAG card by typing:

   ```
   dagrom -d0 -rpy -f dag43ge-ipf.bit
   ```

   **Output**

   ```
   current:        edag43epci_ipf_v2_4 2v1000ff896 2005/11/16 16:55:24 *
   stable:         edag43epci_erf_v2_11 2v1000ff896 2005/04/21 16:22:35
   Card Serial: 4001
   ```

2. Load the IP Filter firmware image for the Co-Processor by typing:

   For the **SC128 Co-Processor**

   ```
   dagld -d0 -x copro-ipf43ge.bit
   ```

   **Output**

   ```
   Waiting for Xilinx1 (ec10gcp_ipf_v2_2 2v2000ff896) to program...
   FPGA Initialized.
   Starting to program
   ................................................
   File loaded.
   Done.
   ```

   For the **SC256 Co-Processor**

   ```
   dagld -d d0 –x copro2-ipf43ge.bit
   ```

   **Output**

   ```
   Waiting for Xilinx1 (ec20gcp_ipf32_cp_v2_5 2v2000ff896) to program ...
   FPGA Initialized.
   Starting to program
   ................................................
   File loaded.
   Done.
   ```

3. Configure DAG card.

   Type the following for an initial configuration:

   ```
   dagfour –d0 default slen=1540
   ```

   **Output**

   ```
   linkA nonic noeql rxpkts txpkts crc long=1518 enablea
   linkB nonic noeql rxpkts txpkts crc long=1518 enableb
   packet varlen slen=1540 align64
   packetA drop=0
   packetB drop=0
   ipf  nodrop steer=steam0
   pcix 133MHz 64-bit buf=128MiB rxstreams=2 txstreams=0 mem=64:0:64:0
   ```

 

## Configure DAG 4.3S Card and Co-Processor

To configure the DAG 4.3S card and Co-Processor, complete the following steps:

**Note:** The DAG 4.3S card has different Co-Processor firmware images for the SC128 and SC256 Co-Processors.

1. Load the IP Filter firmware image for the DAG card by typing:

   ```
   dagrom -d0 –rpy -f dag43s-ipf.bit
   ```

   **Output**

   ```
   current: edag43spcix_ipf_v2_3 2v1000ff896 2005/11/17 15:51:05 *
   stable:  edag43spcix_erf_v2_12 2v1000ff896 2004/04/13 14:53:33
   Card Serial: 3864
   ```

2. Load the IP Filter firmware image for the Co-Processor by typing:

   For the **SC128 Co-Processor**

   ```
   dagld -d0 –x copro-ipf43s.bit
   ```

   **Output**

   ```
   Waiting for Xilinx1 (ec10gcp_ipf32_cp_v2_1 2v2000ff896) to program ...
   FPGA Initialized.
   Starting to program
   ..............................................
   File loaded.
   Done.
   ```

   For the **SC256 Co-Processor**

   ```
   dagld -d0 –x copro2-ipf43s.bit
   Waiting for Xilinx1 (ec20gcp_ipf32_cp_v2_5 2v2000ff896) to program ...
   FPGA Initialized.
   Starting to program
   ................................................
   File loaded.
   Done.
   ```

3. Configure DAG card.

   Type the following for an initial configuration:

   ```
   dagfour -d0 default slen=1540
   ```

   **Output**

   ```
   light   nolaser
   link    noreset OC48c nofcl noeql
   sonet   master scramble
   POS     crc32 nocrcstrip short=16 long=1536 discard pscramble rxpkts txpkts
   packet  varlen slen=1540 align64
   packetA drop=0
   ipf     nodrop steer=colour
   pcix    133MHz 64-bit buf=128MiB rxstreams=2 txstreams=0 mem=64:0:64:0
   ```

**Note:** When using th Co-Processor 2 IPF image with the SC256 Co-Processor the maximum snap length (slen) is 1600 Bytes. Only use variable mength (`varlen`) capture functions.

# Version History

| Version | Date | Reason |
|---|---|---|
| 1-5 | - | Previous versions |
| 6 | March 2006 | - |
| 7 | September 2007 | Addition of 5.2SXA information |
| 8 | January 2008 | Added 5.0SG2A information and corrected minor errors |
| 9 | February 2008 | Updated filter keywords |
| 10 | November 2008 | Removed references to 5.2SXA and 5.0SG2A. This information is going into a new Document. EDM04-26. Moved filter_loader, snort_compiler and tcpdump_compiler information to a new document EDM04-28. |