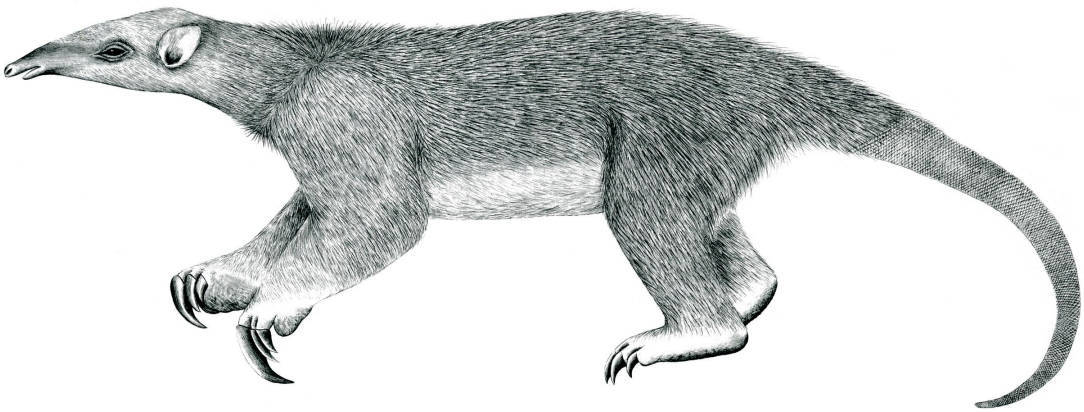
Tranalyzer2

macRecorder

MAC addresses



Tranalyzer Development Team

Contents

1 macRecorder

1.1 Description

The macRecorder plugin provides the source- and destination MAC address as well as the number of packets detected in the flow separated by an underscore. If there is more than one combination of MAC addresses, e.g., due to load balancing or router misconfiguration, the plugin prints all recognized MAC addresses separated by semicolons. The number of distinct source- and destination MAC addresses can be output by activating the `MR_NPAIRS` flag. The `MR_MANUF` flags controls the output of the manufacturers for the source and destination addresses. The representation of MAC addresses can be altered using the `MR_MAC_FMT` flag.

1.2 Dependencies

1.2.1 Required Files

The file `manuf.txt` is required if `MR_MANUF > 0` and file `maclbl.txt` is required if `MR_MACLBL > 0`.

1.3 Configuration Flags

The following flags can be used to control the output of the plugin:

Name	Default	Description	Flags
`MR_MAC_FMT`	1	Format for MAC addresses: 0: hex, 1: mac, 2: int	
`MR_NPAIRS`	1	Report number of distinct MAC/IP pairs	
`MR_MACLBL`	2	Format for MAC addresses labels 0: no labels, 1: numerical (int), 2: short Organization 3: full Organization	
`MR_MAX_MAC`	16	Max number of MAC addresses per flow	
`MR_NO_MANUF`	`"-"`	Representation of unknown manufacturers	

In addition, the following flags can be found in *macLbl.h*:

Name	Default	Description	Flags
`MAC_SORGLEN`	12	Maximum length for 'who' information (short version)	
`MAC_ORGLEN`	44	Maximum length for 'who' information (long version)	

Note that the name of the MAC label file to load can be controlled with `MACLBLFILE` in *macLbl.h*.

1.4 Flow File Output

The macRecorder plugin outputs the following columns:

Column	Type	Description	Flags
macStat	H8	Status	
macPairs	U32	Number of distinct src/dst MAC addresses pairs	MR_NPAIRS=1
srcMac_dstMac_numP	R(H64_H64_U64)	Src/Dst MAC addresses, number of packets	MR_MAC_FMT=0
srcMac_dstMac_numP	R(MAC_MAC_U64)	Src/Dst MAC addresses, number of packets	MR_MAC_FMT=1
srcMac_dstMac_numP	R(U64_U64_U64)	Src/Dst MAC addresses, number of packets	MR_MAC_FMT=2
srcMacLbl_dstMacLbl	R(U32_U32)	Src/Dst MAC label (numerical)	MR_MACLBL=1
srcMacLbl_dstMacLbl	R(SC_SC)	Src/Dst MAC label (string_class)	MR_MACLBL=2
srcMacLbl_dstMacLbl	R(S_S)	Src/Dst MAC label (string)	MR_MACLBL=3

1.4.1 macStat

The macStat column is to be interpreted as follows:

macStat	Description
0x01	MAC list overflow. . . increase MR_MAX_MAC

1.5 Packet File Output

In packet mode (-s option), the macRecorder plugin outputs the following columns:

Column	Type	Description	Flags
srcMacLbl	S	Source MAC label	MR_MACLBL>0
dstMacLbl	S	Destination MAC label	MR_MACLBL>0

1.6 Plugin Report Output

The following information is reported:

- Aggregated macStat
- MAC pairs per flow: min, max, average

1.7 Example Output

Consider a host with MAC address aa:aa:aa:aa:aa:aa in a local network requesting a website from a public server. Due to load balancing, the opposite flow can be split and transmitted via two routers with MAC addresses bb:bb:bb:bb:bb:bb and cc:cc:cc:cc:cc:cc. The macRecorder plugin then produces the following output in default configuration:

```
bb:bb:bb:bb:bb:bb_aa:aa:aa:aa:aa:aa_667;cc:cc:cc:cc:cc:cc_aa:aa:aa:aa:aa:aa_666
```