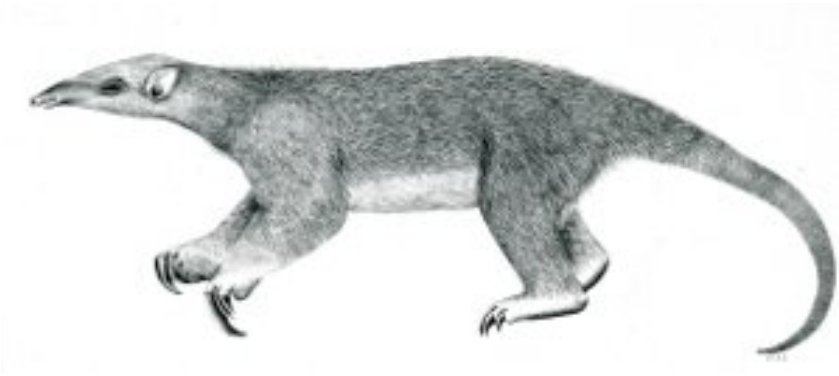
Tranalyzer2

arpDecode

Address Resolution Protocol (ARP)



Tranalyzer Development Team

Contents

1 arpDecode

1.1 Description

The arpDecode plugin analyzes ARP traffic.

1.2 Configuration Flags

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

Name	Default	Description
MAX_IP	10	Max. number of MAC/IP pairs to list

1.3 Flow File Output

The arpDecode plugin outputs the following columns:

Column	Type	Description
arpStat	H8	Status
arpHwType	U16	Hardware type
arpOpcode	H16	Operational code
arpIpMacCnt	U16	Number of distinct MAC / IP pairs
arpMac_Ip_Cnt	MAC_IP4_U16	MAC, IP pairs found and number of times the pair appeared. (a count of zero may appear in case of ARP spoofing and indicates the pair was discovered in a different flow)

1.3.1 arpStat

The arpStat column is to be interpreted as follows:

arpStat	Description
0x01	ARP detected
0x02	MAC/IP list truncated... increase MAX_IP
0x08	Gratuitous ARP (sender IP same as target IP)
0x80	ARP spoofing (same IP assigned to multiple MAC)

1.3.2 arpHwType

The `arpHwType` column is to be interpreted as follows:

Type	Description
1	Ethernet
2	Experimental Ethernet
3	Amateur Radio AX.25
4	Proteon ProNET Token Ring
5	Chaos
6	IEEE 802
7	ARCNET
8	Hyperchannel
9	Lanstar
10	Autonet Short Address
11	LocalTalk
12	LocalNet (IBM PCNet or SYTEK LocalNET)
13	Ultra link
14	SMDS
15	Frame Relay
16	ATM (Asynchronous Transmission Mode)
17	HDLC
18	Fibre Channel

Type	Description
19	ATM (Asynchronous Transmission Mode)
20	Serial Line
21	ATM (Asynchronous Transmission Mode)
22	MIL-STD-188-220
23	Metricom
24	IEEE 1394.1995
25	MAPOS
26	Twinaxial
27	EUI-64
28	HIPARP
29	IP and ARP over ISO 7816-3
30	ARPSec
31	IPsec tunnel
32	Infiniband
33	CAI (TIA-102 Project 25 Common Air Interface)
34	Wiegand Interface
35	Pure IP

1.3.3 arpOpcode

The `arpOpcode` column is to be interpreted as follows:

arpOpcode	Description
2^0 (=0x0001)	—
2^1 (=0x0002)	ARP Request
2^2 (=0x0004)	ARP Reply
2^3 (=0x0008)	Reverse ARP (RARP) Request
2^4 (=0x0010)	Reverse ARP (RARP) Reply
2^5 (=0x0020)	Dynamic RARP (DRARP) Request
2^6 (=0x0040)	Dynamic RARP (DRARP) Reply
2^7 (=0x0080)	Dynamic RARP (DRARP) Error

arpOpcode	Description
2^8 (=0x0100)	Inverse ARP (InARP) Request
2^9 (=0x0200)	Inverse ARP (InARP) Reply
2^{10} (=0x0400)	ARP NAK
2^{11} (=0x0800)	—
2^{12} (=0x1000)	—
2^{13} (=0x2000)	—
2^{14} (=0x4000)	—
2^{15} (=0x8000)	—

1.4 Plugin Report Output

The following information is reported:

- Aggregated status flags (arpStat)

1.5 Packet File Output

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

Column	Description
arpStat	Status
arpHwType	Hardware type
arpProtoType	Protocol type
arpHwSize	Hardware size
arpProtoSize	Protocol size
arpOpcode	Operational code
arpSenderMAC	Sender MAC address
arpSenderIP	Sender IP address
arpTargetMAC	Target MAC address
arpTargetIP	Target IP address