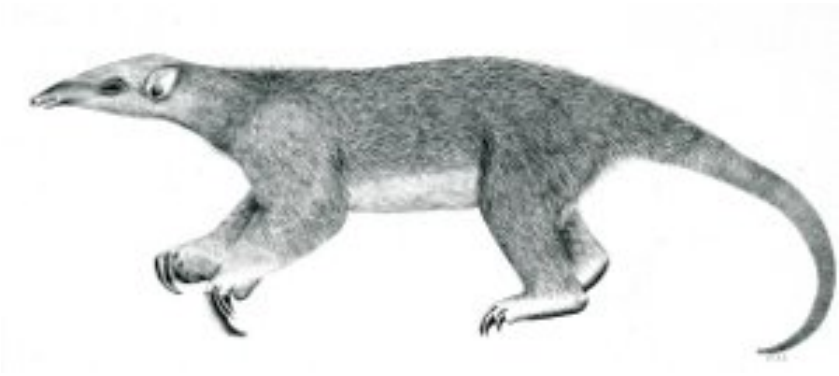
Tranalyzer2

dhcpDecode

Dynamic Host Configuration Protocol (DHCP)



Tranalyzer Development Team

Contents

1 dhcpDecode

1.1 Description

This dhcpDecode plugin analyzes DHCP traffic.

1.2 Configuration Flags

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

Name	Default	Description	Flags
DHCPBITFLD	1	Options representation: 1: bitfield, 0: option numbers in a row	
DHCPMAXOPT	50	maximum stored options	DHCPBITFLD=0
DHCPNMMAX	10	maximal number of domain/host names per flow	
DHCPMASKFRMT	1	Netmask representation: 0: hex, 1: IP	
DHCP_ADD_CNT	0	Print the number of times a given mac/domain/host appeared	
DHCP_FLAG_MAC	0	Store a global mapping IP->MAC and add the source and destination MAC address to every flow [EXPERIMENTAL]	
DHCP_FM_DEBUG	0	print debug information about DHCP_FLAG_MAC operations	

1.3 Flow File Output

The dhcpDecode plugin outputs the following columns:

Column	Type	Description	Flags
dhcpStat	H16	Status, warnings and errors	
dhcpMType	H16/H32	Message type	
dhcpHWType	H32	Hardware Type	
dhcpCHWAdd	R(MAC)	Client hardware addresses	DHCP_ADD_CNT=0
dhcpCHWAdd_HWCnt	R(MAC_H32)	Client hardware addresses and count	DHCP_ADD_CNT=1
If IPV6_ACTIVATE == 0|2, the following columns are output:			
dhcpNetmask	H32/IP4	Network mask	DHCPMASKFRMT=0/1
dhcpGWIP	IP4	Gateway IP	
dhcpDnsIP	IP4	DNS IP	
dhcpHopCnt	H32	Hop Count	
dhcpSrvName	S	Server host name	
dhcpBootFile	S	Boot file name	
dhcpOptCnt	U16	Option Count	
dhcpOpts	RU8	Options	DHCPBITFLD=0
dhcpOptBF1_BF2_BF3	H64_H64_H64	Option Bit field	DHCPBITFLD=1
dhcpHosts	R(S)	Maximal DHCPNMMAX hosts	DHCP_ADD_CNT=0
dhcpHosts_HCnt	R(S_U16)	Maximal DHCPNMMAX hosts and count	DHCP_ADD_CNT=1
dhcpDomains	R(S)	Maximal DHCPNMMAX domains	DHCP_ADD_CNT=0
dhcpDomains_DCnt	R(S_U16)	Maximal DHCPNMMAX domains and count	DHCP_ADD_CNT=1
dhcpMaxSecEl	U16	Maximum seconds elapsed	

Column	Type	Description	Flags
dhcpLeaseT	U32	Lease time	
dhcpRenewT	U32	Renewal time	
dhcpRebindT	U32	Rebind time	
dhcpCliIP	IP4	DHCP client IP	
dhcpYourIP	IP4	DHCP your (client) IP	
dhcpNextServer	IP4	DHCP next server IP	
dhcpRelay	IP4	DHCP relay agent IP	
dhcpLFlow	U64	DHCP linked flow	
dhcpSrcMac	MAC	DHCP source MAC address	DHCP_FLAG_MAC=1
dhcpDstMac	MAC	DHCP destination MAC address	DHCP_FLAG_MAC=1

1.3.1 dhcpStat

The dhcpStat status bit field is to be interpreted as follows:

dhcpStat	Description
0x0001	DHCP detected
0x0002	Boot request
0x0004	Boot reply
0x0008	Broadcast
0x0010	Client ID (option 61) different from Client MAC address
0x0020	Option overload: server host name and/or boot file name carry options
0x0100	Option list truncated... increase DHCPMAXOPT
0x0200	Client HW address, domain or host name list truncated... increase DHCPNMMAX
0x2000	Error: DHCP magic number corrupt
0x4000	Error: DHCP options corrupt
0x8000	Something weird happened...

1.3.2 dhcpMType

For IPv4, the dhcpMType column is to be interpreted as follows:

dhcpMType4	Description
2^1 (=0x0002)	Discover Message
2^2 (=0x0004)	Offer Message
2^3 (=0x0008)	Request Message
2^4 (=0x0010)	Decline Message
2^5 (=0x0020)	Acknowledgment Message
2^6 (=0x0040)	Negative Acknowledgment Message
2^7 (=0x0080)	Release Message
2^8 (=0x0100)	Informational Message

For IPv6, the dhcpMType column is to be interpreted as follows:

dhcpMType6	Description
0x0000 0001	Reserved
0x0000 0002	SOLICIT
0x0000 0004	ADVERTISE
0x0000 0008	REQUEST
0x0000 0010	CONFIRM
0x0000 0020	RENEW
0x0000 0040	REBIND
0x0000 0080	REPLY
0x0000 0100	RELEASE
0x0000 0200	DECLINE
0x0000 0400	RECONFIGURE
0x0000 0800	INFORMATION-REQUEST

dhcpMType6	Description
0x0000 1000	RELAY-FORW
0x0000 2000	RELAY-REPL
0x0000 4000	LEASEQUERY
0x0000 8000	LEASEQUERY-REPLY
0x0001 0000	LEASEQUERY-DONE
0x0002 0000	LEASEQUERY-DATA
0x0004 0000	RECONFIGURE-REQUEST
0x0008 0000	RECONFIGURE-REPLY
0x0010 0000	DHCPV4-QUERY
0x0020 0000	DHCPV4-RESPONSE
0x0040 0000	ACTIVELEASEQUERY
0x0080 0000	STARTTLS

1.3.3 dhcpHWType

The dhcpHWType column is to be interpreted as follows:

dhcpHWType	Description
2^0 (=0x0000 0000 0000 0001)	—
2^1 (=0x0000 0000 0000 0002)	Ethernet
2^2 (=0x0000 0000 0000 0004)	Experimental Ethernet
2^3 (=0x0000 0000 0000 0008)	Amateur Radio AX.25
2^4 (=0x0000 0000 0000 0010)	Proteon ProNET Token Ring
2^5 (=0x0000 0000 0000 0020)	Chaos
2^6 (=0x0000 0000 0000 0040)	IEEE 802
2^7 (=0x0000 0000 0000 0080)	ARCNET
2^8 (=0x0000 0000 0000 0100)	Hyperchannel
2^9 (=0x0000 0000 0000 0200)	Lanstar
2^{10} (=0x0000 0000 0000 0400)	Autonet Short Address
2^{11} (=0x0000 0000 0000 0800)	LocalTalk
2^{12} (=0x0000 0000 0000 1000)	LocalNet (IBM PCNet or SYTEK LocalNET)
2^{13} (=0x0000 0000 0000 2000)	Ultra link
2^{14} (=0x0000 0000 0000 4000)	SMDS
2^{15} (=0x0000 0000 0000 8000)	Frame Relay
2^{16} (=0x0000 0000 0001 0000)	ATM, Asynchronous Transmission Mode
2^{17} (=0x0000 0000 0002 0000)	HDLC
2^{18} (=0x0000 0000 0004 0000)	Fibre Channel
2^{19} (=0x0000 0000 0008 0000)	ATM, Asynchronous Transmission Mode
2^{20} (=0x0000 0000 0010 0000)	Serial Line
2^{21} (=0x0000 0000 0020 0000)	ATM, Asynchronous Transmission Mode
2^{22} (=0x0000 0000 0040 0000)	MIL-STD-188-220
2^{23} (=0x0000 0000 0080 0000)	Metricom
2^{24} (=0x0000 0000 0100 0000)	IEEE 1394.1995
2^{25} (=0x0000 0000 0200 0000)	MAPOS

dhcpHWType	Description
2^{26} (=0x0000 0000 0400 0000)	Twinaxia
2^{27} (=0x0000 0000 0800 0000)	EUI-64
2^{28} (=0x0000 0000 1000 0000)	HIPARP
2^{29} (=0x0000 0000 2000 0000)	IP and ARP over ISO 7816-3
2^{30} (=0x0000 0000 4000 0000)	ARPSec
2^{31} (=0x0000 0000 8000 0000)	IPsec tunnel
2^{32} (=0x0000 0001 0000 0000)	Infiniband
2^{33} (=0x0000 0002 0000 0000)	CAI, TIA-102 Project 25 Common Air Interface
2^{34} (=0x0000 0004 0000 0000)	Wiegand Interface
2^{35} (=0x0000 0008 0000 0000)	Pure IP
2^{63} (=0x8000 0000 0000 0000)	All values bigger than 62 are reported here

1.3.4 dhcpHopCnt

The dhcpHopCnt column is to be interpreted as follows:

dhcpHopCnt	Description
0x00000000-0x00010000	Number of hops (0–16) $\left(2^{\text{HopCount}}\right)$
0x80000000	Invalid hop count (> 16)

1.3.5 dhcpOptBF1_BF2_BF3

The dhcpOptBF1_BF2_BF3 column is to be interpreted as follows:

dhcpOptBF1	Length	Description
2^{0} (=0x0000.0000.0000.0001)	0	Pad
2^{1} (=0x0000.0000.0000.0002)	4	Subnet Mask
2^{2} (=0x0000.0000.0000.0004)	4	Time Offset (deprecated)
2^{3} (=0x0000.0000.0000.0008)	4+	Router
2^{4} (=0x0000.0000.0000.0010)	4+	Time Server
2^{5} (=0x0000.0000.0000.0020)	4+	Name Server
2^{6} (=0x0000.0000.0000.0040)	4+	Domain Name Server
2^{7} (=0x0000.0000.0000.0080)	4+	Log Server
2^{8} (=0x0000.0000.0000.0100)	4+	Quote Server
2^{9} (=0x0000.0000.0000.0200)	4+	LPR Server
2^{10} (=0x0000.0000.0000.0400)	4+	Impress Server
2^{11} (=0x0000.0000.0000.0800)	4+	Resource Location Server
2^{12} (=0x0000.0000.0000.1000)	1+	Host Name
2^{13} (=0x0000.0000.0000.2000)	2	Boot File Size
2^{14} (=0x0000.0000.0000.4000)	1+	Merit Dump File
2^{15} (=0x0000.0000.0000.8000)	1+	Domain Name
2^{16} (=0x0000.0000.0001.0000)	4	Swap Server
2^{17} (=0x0000.0000.0002.0000)	1+	Root Path
2^{18} (=0x0000.0000.0004.0000)	1+	Extensions Path
2^{19} (=0x0000.0000.0008.0000)	1	IP Forwarding enable/disable

dhcpOptBF1	Length	Description
2^{20} (=0x0000.0000.0010.0000)	1	Non-local Source Routing enable/disable
2^{21} (=0x0000.0000.0020.0000)	8+	Policy Filter
2^{22} (=0x0000.0000.0040.0000)	2	Maximum Datagram Reassembly Size
2^{23} (=0x0000.0000.0080.0000)	1	Default IP Time-to-live
2^{24} (=0x0000.0000.0100.0000)	4	Path MTU Aging Timeout
2^{25} (=0x0000.0000.0200.0000)	2+	Path MTU Plateau Table
2^{26} (=0x0000.0000.0400.0000)	2	Interface MTU
2^{27} (=0x0000.0000.0800.0000)	1	All Subnets are Local
2^{28} (=0x0000.0000.1000.0000)	4	Broadcast Address
2^{29} (=0x0000.0000.2000.0000)	1	Perform Mask Discovery
2^{30} (=0x0000.0000.4000.0000)	1	Mask supplier
2^{31} (=0x0000.0000.8000.0000)	1	Perform router discovery
2^{32} (=0x0000.0001.0000.0000)	4	Router solicitation address
2^{33} (=0x0000.0002.0000.0000)	8+	Static routing table
2^{34} (=0x0000.0004.0000.0000)	1	Trailer encapsulation
2^{35} (=0x0000.0008.0000.0000)	4	ARP cache timeout
2^{36} (=0x0000.0010.0000.0000)	1	Ethernet encapsulation
2^{37} (=0x0000.0020.0000.0000)	1	Default TCP TTL
2^{38} (=0x0000.0040.0000.0000)	4	TCP keepalive interval
2^{39} (=0x0000.0080.0000.0000)	1	TCP keepalive garbage
2^{40} (=0x0000.0100.0000.0000)	1+	Network Information Service Domain
2^{41} (=0x0000.0200.0000.0000)	4+	Network Information Servers
2^{42} (=0x0000.0400.0000.0000)	4+	NTP servers
2^{43} (=0x0000.0800.0000.0000)	1+	Vendor specific information
2^{44} (=0x0000.1000.0000.0000)	4+	NetBIOS over TCP/IP name server
2^{45} (=0x0000.2000.0000.0000)	4+	NetBIOS over TCP/IP Datagram Distribution Server
2^{46} (=0x0000.4000.0000.0000)	1	NetBIOS over TCP/IP Node Type
2^{47} (=0x0000.8000.0000.0000)	1+	NetBIOS over TCP/IP Scope
2^{48} (=0x0001.0000.0000.0000)	4+	X Window System Font Server
2^{49} (=0x0002.0000.0000.0000)	4+	X Window System Display Manager
2^{50} (=0x0004.0000.0000.0000)	4	Requested IP Address
2^{51} (=0x0008.0000.0000.0000)	4	IP address lease time
2^{52} (=0x0010.0000.0000.0000)	4	Option overload
2^{53} (=0x0020.0000.0000.0000)	4	DHCP message type
2^{54} (=0x0040.0000.0000.0000)	1	Server identifier
2^{55} (=0x0080.0000.0000.0000)	1+	Parameter request list
2^{56} (=0x0100.0000.0000.0000)	1+	Message
2^{57} (=0x0200.0000.0000.0000)	2	Maximum DHCP message size
2^{58} (=0x0400.0000.0000.0000)	4	Renew time value
2^{59} (=0x0800.0000.0000.0000)	4	Rebinding time value
2^{60} (=0x1000.0000.0000.0000)	1+	Class-identifier
2^{61} (=0x2000.0000.0000.0000)	2+	Client-identifier
2^{62} (=0x4000.0000.0000.0000)	1-255	NetWare/IP Domain Name
2^{63} (=0x8000.0000.0000.0000)	1	NetWare/IP information

dhcpOptBF2	Length	Description
2^{64} (=0x0000.0000.0000.0001)	1+	Network Information Service+ Domain
2^{65} (=0x0000.0000.0000.0002)	4+	Network Information Service+ Servers

dhcpOptBF2	Length	Description
2^{66} (=0x0000.0000.0000.0004)	1+	TFTP server name
2^{67} (=0x0000.0000.0000.0008)	1+	Bootfile name
2^{68} (=0x0000.0000.0000.0010)	0+	Mobile IP Home Agen
2^{69} (=0x0000.0000.0000.0020)	4+	Simple Mail Transport Protocol Server
2^{70} (=0x0000.0000.0000.0040)	4+	Post Office Protocol Server
2^{71} (=0x0000.0000.0000.0080)	4+	Network News Transport Protocol Server
2^{72} (=0x0000.0000.0000.0100)	4+	Default World Wide Web Server
2^{73} (=0x0000.0000.0000.0200)	4+	Default Finger Server
2^{74} (=0x0000.0000.0000.0400)	4+	Default Internet Relay Chat Server
2^{75} (=0x0000.0000.0000.0800)	4+	StreetTalk Server
2^{76} (=0x0000.0000.0000.1000)	4+	StreetTalk Directory Assistance Server
2^{77} (=0x0000.0000.0000.2000)	0-255	User Class Information
2^{78} (=0x0000.0000.0000.4000)	0-255	SLP Directory Agent
2^{79} (=0x0000.0000.0000.8000)	0-255	SLP Service Scope
2^{80} (=0x0000.0000.0001.0000)	0	Rapid Commit
2^{81} (=0x0000.0000.0002.0000)	4+	FQDN, Fully Qualified Domain Name
2^{82} (=0x0000.0000.0004.0000)	0-255	Relay Agent Information
2^{83} (=0x0000.0000.0008.0000)	14+	Internet Storage Name Service
2^{84} (=0x0000.0000.0010.0000)	—	—
2^{85} (=0x0000.0000.0020.0000)	8+	—
2^{86} (=0x0000.0000.0040.0000)	2	—
2^{87} (=0x0000.0000.0080.0000)	1	—
2^{88} (=0x0000.0000.0100.0000)	4	—
2^{89} (=0x0000.0000.0200.0000)	2+	—
2^{90} (=0x0000.0000.0400.0000)	2	—
2^{91} (=0x0000.0000.0800.0000)	1	—
2^{92} (=0x0000.0000.1000.0000)	4	—
2^{93} (=0x0000.0000.2000.0000)	1	—
2^{94} (=0x0000.0000.4000.0000)	1	—
2^{95} (=0x0000.0000.8000.0000)	1	—
2^{96} (=0x0000.0001.0000.0000)	—	—
2^{97} (=0x0000.0002.0000.0000)	—	—
2^{98} (=0x0000.0004.0000.0000)	—	—
2^{99} (=0x0000.0008.0000.0000)	—	—
2^{100} (=0x0000.0010.0000.0000)	—	—
2^{101} (=0x0000.0020.0000.0000)	—	—
2^{102} (=0x0000.0040.0000.0000)	—	—
2^{103} (=0x0000.0080.0000.0000)	—	—
2^{104} (=0x0000.0100.0000.0000)	1+	—
2^{105} (=0x0000.0200.0000.0000)	—	—
2^{106} (=0x0000.0400.0000.0000)	—	—
2^{107} (=0x0000.0800.0000.0000)	—	—
2^{108} (=0x0000.1000.0000.0000)	—	—
2^{109} (=0x0000.2000.0000.0000)	—	—
2^{110} (=0x0000.4000.0000.0000)	—	—
2^{111} (=0x0000.8000.0000.0000)	—	—
2^{112} (=0x0001.0000.0000.0000)	—	—
2^{113} (=0x0002.0000.0000.0000)	—	—
2^{114} (=0x0004.0000.0000.0000)	—	—

dhcpOptBF2	Length	Description
2^{115} (=0x0008.0000.0000.0000)	—	—
2^{116} (=0x0010.0000.0000.0000)	—	—
2^{117} (=0x0020.0000.0000.0000)	—	—
2^{118} (=0x0040.0000.0000.0000)	—	—
2^{119} (=0x0080.0000.0000.0000)	—	—
2^{120} (=0x0100.0000.0000.0000)	—	—
2^{121} (=0x0200.0000.0000.0000)	5+	—
2^{122} (=0x0400.0000.0000.0000)	0-255	—
2^{123} (=0x0800.0000.0000.0000)	16	—
2^{124} (=0x1000.0000.0000.0000)	—	—
2^{125} (=0x2000.0000.0000.0000)	—	—
2^{126} (=0x4000.0000.0000.0000)	—	—
2^{127} (=0x8000.0000.0000.0000)	—	—

dhcpOptBF3	Length	Description
2^{128} (=0x0000.0000.0000.0001)	—	TFTP Server IP address
2^{129} (=0x0000.0000.0000.0002)	—	Call Server IP addres
2^{130} (=0x0000.0000.0000.0004)	—	Discrimination string
2^{131} (=0x0000.0000.0000.0008)	—	Remote statistics server IP address
2^{132} (=0x0000.0000.0000.0010)	—	802.1P VLAN ID
2^{133} (=0x0000.0000.0000.0020)	—	802.1Q L2 Priority
2^{134} (=0x0000.0000.0000.0040)	—	Diffserv Code Point
2^{135} (=0x0000.0000.0000.0080)	—	HTTP Proxy for phone-specific applications
2^{136} (=0x0000.0000.0000.0100)	4+	PANA Authentication Agent
2^{137} (=0x0000.0000.0000.0200)	0-255	LoST Server
2^{138} (=0x0000.0000.0000.0400)	—	CAPWAP Access Controller addresses
2^{139} (=0x0000.0000.0000.0800)	—	OPTION-IPv4_Address-MoS
2^{140} (=0x0000.0000.0000.1000)	—	OPTION-IPv4_FQDN-MoS
2^{141} (=0x0000.0000.0000.2000)	2+	SIP UA Configuration Service Domains
2^{142} (=0x0000.0000.0000.4000)	—	OPTION-IPv4_Address-ANDSF
2^{143} (=0x0000.0000.0000.8000)	—	OPTION-IPv6_Address-ANDSF
2^{144} (=0x0000.0000.0001.0000)	—	—
2^{145} (=0x0000.0000.0002.0000)	—	—
2^{146} (=0x0000.0000.0004.0000)	—	—
2^{147} (=0x0000.0000.0008.0000)	—	—
2^{148} (=0x0000.0000.0010.0000)	—	—
2^{149} (=0x0000.0000.0020.0000)	—	—
2^{150} (=0x0000.0000.0040.0000)	—	TFTP server address or Etherboot-GRUB configuration path name
2^{151} (=0x0000.0000.0080.0000)	—	status-code
2^{152} (=0x0000.0000.0100.0000)	—	base-time
2^{153} (=0x0000.0000.0200.0000)	—	start-time-of-state
2^{154} (=0x0000.0000.0400.0000)	—	query-start-time
2^{155} (=0x0000.0000.0800.0000)	—	query-end-time
2^{156} (=0x0000.0000.1000.0000)	—	dhcp-state
2^{157} (=0x0000.0000.2000.0000)	—	data-source
2^{158} (=0x0000.0000.4000.0000)	—	—
2^{159} (=0x0000.0000.8000.0000)	—	—
2^{160} (=0x0000.0001.0000.0000)	—	—

dhcpOptBF3	Length	Description
2^{161} (=0x0000.0002.0000.0000)	—	—
2^{162} (=0x0000.0004.0000.0000)	—	—
2^{163} (=0x0000.0008.0000.0000)	—	—
2^{164} (=0x0000.0010.0000.0000)	—	—
2^{165} (=0x0000.0020.0000.0000)	—	—
2^{166} (=0x0000.0040.0000.0000)	—	—
2^{167} (=0x0000.0080.0000.0000)	—	—
2^{168} (=0x0000.0100.0000.0000)	—	—
2^{169} (=0x0000.0200.0000.0000)	—	—
2^{170} (=0x0000.0400.0000.0000)	—	—
2^{171} (=0x0000.0800.0000.0000)	—	—
2^{172} (=0x0000.1000.0000.0000)	—	—
2^{173} (=0x0000.2000.0000.0000)	—	—
2^{174} (=0x0000.4000.0000.0000)	—	—
2^{175} (=0x0000.8000.0000.0000)	—	Etherboot
2^{176} (=0x0001.0000.0000.0000)	—	IP Telephone
2^{177} (=0x0002.0000.0000.0000)	—	Etherboot, PacketCable and CableHome
2^{178} (=0x0004.0000.0000.0000)	—	—
2^{179} (=0x0008.0000.0000.0000)	—	—
2^{180} (=0x0010.0000.0000.0000)	—	—
2^{181} (=0x0020.0000.0000.0000)	—	—
2^{182} (=0x0040.0000.0000.0000)	—	—
2^{183} (=0x0080.0000.0000.0000)	—	—
2^{184} (=0x0100.0000.0000.0000)	—	—
2^{185} (=0x0200.0000.0000.0000)	—	—
2^{186} (=0x0400.0000.0000.0000)	—	—
2^{187} (=0x0800.0000.0000.0000)	—	—
2^{188} (=0x1000.0000.0000.0000)	—	—
2^{189} (=0x2000.0000.0000.0000)	—	—
2^{190} (=0x4000.0000.0000.0000)	—	—
2^{191} (=0x8000.0000.0000.0000)	—	—

1.4 Packet File Output

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

Column	Type	Description
dhcpMType	U8	Message type
dhcpHops	U8	Number of hops
dhcpTransID	U16	Transaction Identifier
dhcpLFlow	U16	Linked flow

1.5 Plugin Report Output

The number of DHCP packets of each type (Section 1.3.2) is reported.

1.6 TODO

- DHCPv6

1.7 References

- RFC2131: Dynamic Host Configuration Protocol
- RFC2132: DHCP Options and BOOTP Vendor Extensions