

**NAME**

trawl – Snoop and record DHCP traffic.

**SYNOPSIS**

**trawl** [-f] [-v] [-dn ] [-i *interface1 interface2...* ]

**DESCRIPTION**

**trawl**, which must be invoked by **root**, runs as a UNIX daemon process and is intended to accumulate statistics about DHCP traffic. The statistics of each DHCP client are accumulated independantly.

**trawl** spies on DHCP packets and captures information about the correspondence between the hardware addresses, hostnames, and various other data fields of interest. Counts of the number of DHCP messages of particular types (discovers, requests, releases etc) are maintained. This data is keyed from the client's hardware address and is stored in a hash file, **dbz.hsh** in the JOINSPOOL directory. The data in this hash may be dumped as text strings using a companion utility **jdbz(1)**.

During the lifetime of a particular **trawl** invocation, dhcp clients may send and receive multiple packets. The counters are incremented for each packet type, but only a single value for the other data is maintained. This data is only updated when packets are received from the client, and only when that data is present and valid. For instance, when a client lying on the remote side of a DHCP relay agent initially acquires an IP address, the **giaddr** will be the IP address of one of the relay's interfaces. Later, if the client renews the IP address, the **giaddr** will be *0.0.0.0*. Only in the former case will the value recorded in **dbz.hsh** be updated.

The data in **dbz.hsh** is not cleared when **trawl** starts so it should be manually removed if fresh statistics are required.

**trawl** is not integral to the operation of DHCP and it isn't necessary that it be run in order to service DHCP clients. In fact, it may be undesirable to do so as it will steal processor cycle from the DHCP server daemon. However, it will not have any other effect; both executables may be run simultaneously.

**trawl**, when run as a daemon, writes a log file **trawl.log** in JOINSPOOL. When the debug level is raised (not recommended for extended operation) summary details of all packets received is logged.

**OPTIONS**

- f           Foreground mode. In this mode **trawl** will not run as a daemon. All debug and other output is sent to stdout and stderr,
- dn           Set debug level to *n*. The volume of output generated by increasing this level is not especially well defined, and may be subject to change without notice. Turning debug on will cause **trawl** to spend time writing the log, and hamper its ability to capture packets.
- i *interface1...*   Don't listen for packets on the interface(s) specified. Normally **trawl** listens for traffic on all network interfaces configured. This option may be used to specify one or more interfaces which it is to ignore. Any traffic on those interfaces will not be captured.
- v           Display the version number and exit.

**DATA CAPTURED**

The following data fields are captured and stored in the hash file:

*HW identifier.*

The hardware address of the client as sent in the DHCP *chaddr* field.

*DHCP Identifier*

DHCP option#61 as sent by the client to the server.

*Hostname*

DHCP option#12 as sent by the client to the server.

*IP address*

The DHCP conferred IP address in use by the client.

*Giaddr*

The IP address of the agent that initially relayed the broadcast packet as contained in the *giaddr* field of the DHCP packet.

*Counters*

Counts of the various DHCP message types sent by/to the client:

- Discovers
- Requests
- Declines
- Releases
- Informs
- LeaseQueries
- Bootp Requests
- Selecting Requests
- Renewing Requests
- Rebinding Requests
- Rebooting Requests
- Offers
- Acks
- Bootp Replies
- Nacks
- Other Message Types (unknowns)

*Timestamp*

The time (in UCT seconds) when this data record was last updated. This will be the same as the last time that the client sent a DHCPREQUEST message from the *selecting* or *init-reboot* state.

*Vendor Class*

DHCP option#60 as sent by the client to the server.

*Relay Agent Information*

DHCP option#82 as inserted into the initially-broadcast DHCP packet by the relaying agent. See RFC3046

**FILES**

**\$JOINSPOOL/rawl.log**  
**\$JOINSPOOLjdbz.hsh**

**SEE ALSO**

**jdbz(1).**  
**RFC3046**