BRNO UNIVERSITY OF TECHNOLOGY
FACULTY OF INFORMATION TECHNOLOGY

Network Applications and Network Administration – Project

DHCP-stats Manual

November 4, 2023

Michal L'aš (xlasmi00)

Contents

1 Introduction

This introduction provides essential information necessary for comprehending the functioning of the dhcp-stats tool. For a thorough understanding of the complex operations of the DHCP protocol, see [2].

The Dynamic Host Configuration Protocol (DHCP) provides a framework for passing configuration information to hosts on a TCP/IP network. DHCP is providing two services:

1. it is delivering host-specific configuration parameters
2. it is assigning network addresses to its hosts

DHCP is built on a client-server model, where designated DHCP server is a host that allocate network addresses and deliver configuration parameters to other network hosts.[2]
The number of addresses that the server can allocate is limited, therefore each DHCP server must keep records of the allocated addresses. In case of allocation of all the addresses the DHCP server should notify the administrator. This is also the main purpose of **dhcp-stats** tool 2.

1.1 The DHCP Packet Header

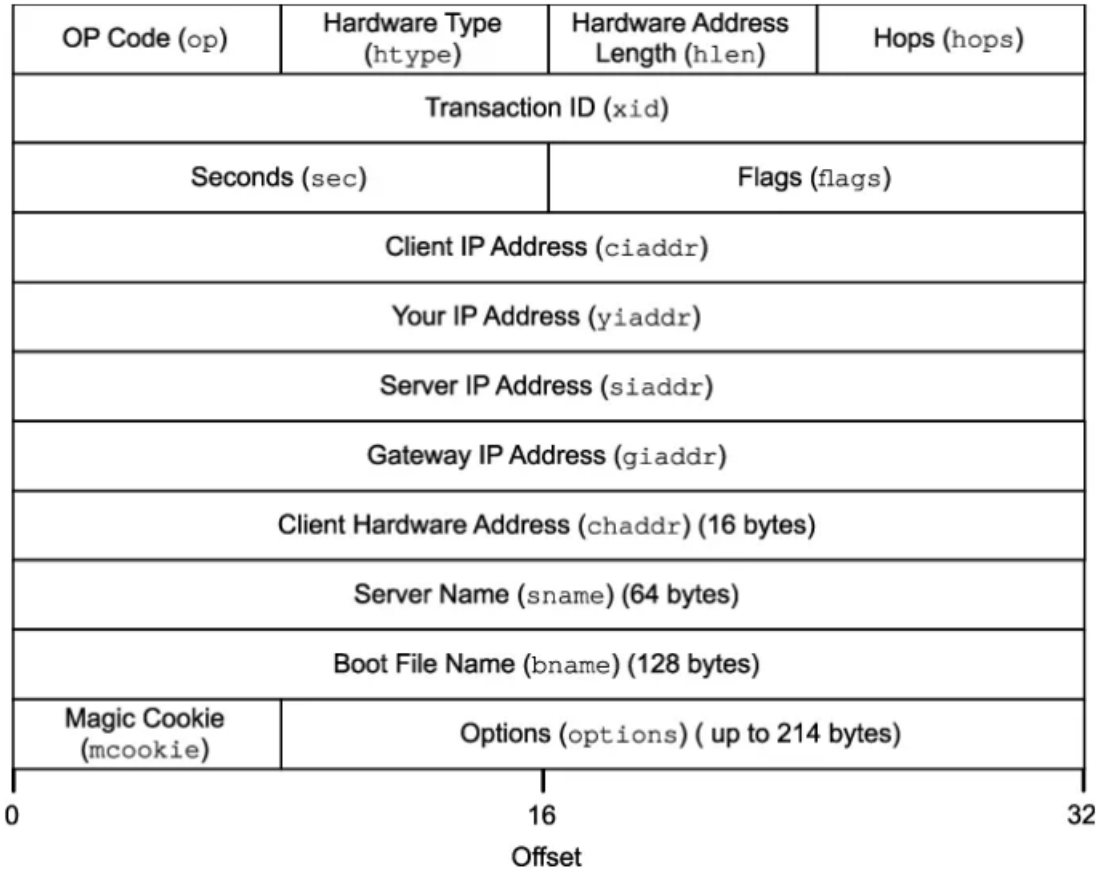

Figure 1: Structure of DHCP packet (figure from: [1])

1.2 DHCP Messages:

DHCP discover message

This is the first message in DHCP communication. The client broadcasts a DHCP discover message without knowing its IP address. The desticantion MAC address is also broadcasts address (FF:FF:FF:FF:FF:FF).

DHCP offers a message

DHCP offer is server's response to DHCP discover message. In this message, server offers ip address to the client. This message is delivered to client based on its MAC address, that was in the DHCP request message. The offered IP address is in `yiaddr` field of DHCP packet.

DHCP request message

When the client recives the DHCP offer message, it response with broadcasting DHCP request message. In the DHCP header of this message in option `Requested IP Address` is IP address that client is requesting from the server.

DHCP acknowledgment message

This message is sent to the client as a positive response to the DHCP request. The server binds the IP address to the client ID. Now, the client has the IP address provided by the DHCP server. The given IP address is in `yiaddr` field of the DHCP packet. The options of this packet contains other useful information for the client, for example `lease time` etc. The DHCP acknowledgment message is also sent in response to a DHCP inform, but it differs from the DHCP acknowledgment in response to a DHCP request in that it cannot include the `lease time` option.

DHCP negative acknowledgment message

This message is sent to the client as a negative response to the DHCP request. Upon receiving this message, the client must initiate the process of obtaining an IP address from the DHCP server once again.

DHCP decline

If the client that received the IP address from the DHCP server discovers that the provided IP address is invalid, it sends a DHCP decline message to the server.

DHCP release

If the client no longer needs the assigned IP address, it sends a DHCP release message. This message signifies that the client's IP address will no longer be in use.

DHCP inform

This message is employed when the client has obtained an IP address manually. The DHCP inform is sent to the server, and in response, the server sends a DHCP acknowledgment message containing local configuration details

1.3 How to track allocated addresses

To track allocated addresses, monitor DHCPACK packets containing the `Lease Time` option. These packets reveal IP addresses assigned by the DHCP server. If a client sends a DHCPDECLINE message, remove that address from the records. Similarly, if a client sends a DHCPRELEASE message, remove the corresponding address from the statistics. Additionally, if the server responds to a DHCPREQUEST message with DHCPNAK because a client attempted to extend its `Lease Time`, remove the address from the statistics.

2 Aplication design

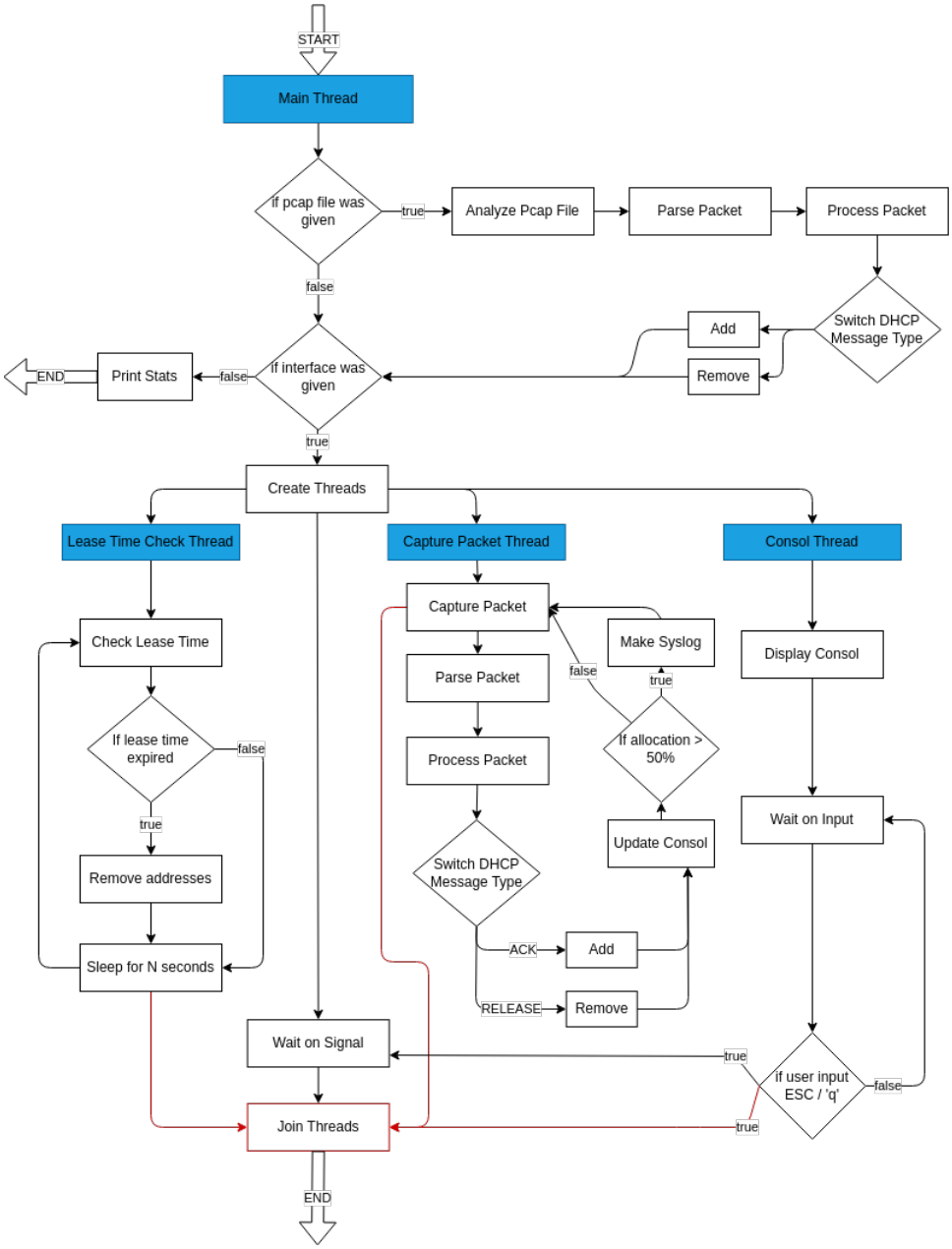

Figure 2: Graph of program operations

Figure 2 outlines the primary operations of the program. It is important to note that the first step is processing the program arguments. Only after the argument processing stage, the operations detailed in figure 2 are executed.

When a pcap file is specified, it takes precedence in processing. If an Internet interface is also provided, the program begins network monitoring on the specified interface after processing the file. If the Internet interface is not specified in the program's arguments, the program outputs statistics to stdout and finishes its operation. Before the packet capture starts, three threads are initiated. The `Lease Time Check Thread` periodically verifies lease time expiration for all allocated IP addresses. If

the lease time has expired for an IP address, it is removed from the list of allocated addresses. The `Console Thread` displays statistics in the console. Upon entering `q` or `ESC` into the console, a stop signal is sent, prompting the program to finish. The `Capture Packet Thread` captures and processes packets, executing actions such as adding or removing an IP address from the statistics based on the packet DHCP message type. After each add/remove action, the method in the 'Consol-Log' class is invoked, updating the displayed data. The red arrows indicate the places from where the threads are connected again after receiving the stop signal.

3 Implementation description

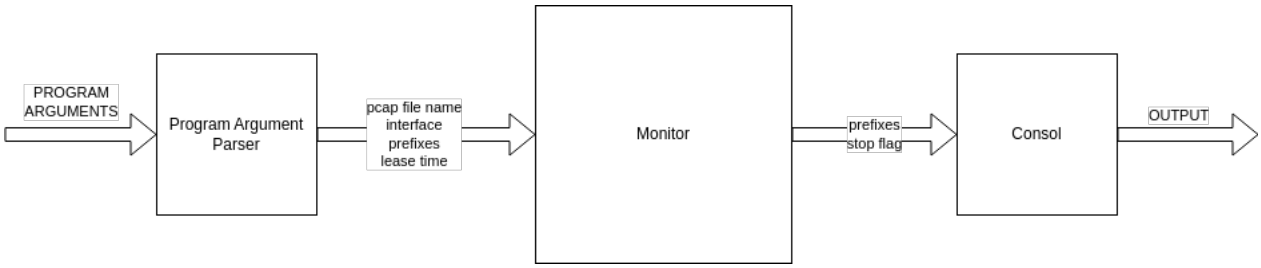

Figure 3: DHCP-stats application components

This program consists of three main components:

- **ArgParser:** This component is responsible for processing program arguments. It contains a `parse()` method that processes and returns the arguments entered during the program's startup. Additionally, this component validates whether all required arguments were provided and checks the validity of the arguments.
- **DHCPMonitor:** Serving as the backbone of the application, this component handles network monitoring, DHCP packet processing, and pcap file analysis (if specified in the program arguments). The `analyze()` method first processes the pcap file and subsequently monitors the network and processing packets on the chosen interface. The more detailed description of the Monitor is in figure 2
- **ConsolLog:** This component manages the display of information related to selected prefixes. If a prefix exceeds the limit of 50% of allocated addresses, ConsolLog records this information in the syslog.

Each prefix is represented by an instance of the IPv4Prefix class. This class contains methods for working with prefixes and stores the number of allocated addresses for a given prefix. An IPv4 address is represented as a 32 bit unsigned integer (`unit32_t`). The `UINT2IP()` and `IP2UINT()` methods are used to convert IPv4 addresses into string form and back.

4 Application brief

This program allows retrieving information about network prefix utilization in terms of allocated IP addresses. Upon execution, the program begins monitoring DHCP traffic on the selected interface or processes a specified pcap file. It generates statistics on the utilization of the network prefix provided in the command line. When the prefix is filled to more than **50%**, the tool notifies the administrator and creates a log using a syslog server.

4.1 Functionality

This application specifically monitors DHCP acknowledgment and DHCP release packets. When processing a DHCPACK packet, a new IP address is allocated within the corresponding prefixes. Upon receiving a DHCPRELEASE packet, the sender's (source) IP address is removed from the list of allocated addresses. If DHCP acknowledgment is received for already allocate IP address, then only lease time of IP address is updated.

The application requires either a pcap file that it analyzes or an network interface on which it will monitor DHCP packets. If both the pcap file and the network interface are specified in the program arguments, then after processing the pcap file, the application continues processing packets on the specified network interface.

The lease time is checked for packets in the pcap file only when the network interface is specified in the program arguments. Lease time for network communication is always checked. This approach ensures that the monitored communication statistics remain current. Additionally, it allows for the analysis of older DHCP communication statistics. If the lease time of the IP address has expired, the IP address is removed from the list of allocated IP addresses.

4.2 Limitations

If the client responds to the DHCPACK message with a DHCPDECLINE message, the IP address will still remain allocated. Consequently, the prefixes associated with this address will continue to include it in the statistics.

If a DHCPNAK message is sent in response to a DHCPREQUEST message intended to renew the lease time of the IP address, the IP address will persist in allocation. Consequently, the prefixes to which this address belongs will continue to include it in the statistics.

If the DHCP packet contains the `option overload`, incorrect processing of the packet may occur, especially if the `message type` and `lease time` options fall outside the standard options field in the DHCP packet.

Logs and warning messages are created only if network interface is specified. This is because it make no sense to create logs or send warning messages during just pcap file analysis. However, if network interface is specified in program arguments then warning notifications from pcap file analysis are printed to `stdout` and notifications from network analysis are printed to program **console**.

This program can proccess packets that are structured only like this:
`Ethernet header` + `IPv4 header` + `UDP header` + `DHCP header`.

4.3 Requirements

- C++ compiler
- Standard C++ libraries
- pcap library
- NCURSES library
- Syslog library

5 Program arguments

`./dhcp-stats ...`

To print information about porgram usage use single argument `-h` or `--help`
Required program arguments:

- `[-i <interface> | --interface <interface>]`: Specifies the network interface where the dhcp-stats tool will monitor DHCP packets. If a single `-i | --interface` argument is provided, the application will list available interfaces
- `[-r <pcap-file> | --read <pcap-file>]` Pcap file from where dhcp-stats tool can read previously monitored DHCP traffic
- `<ip-prefix> [ <ip-prefix> [ ... ]]` IPv4 prefixes that will be monitored

Optional program arguments:

- `[-t <seconds> | --lctime <seconds>]` Frequency of lease time check for monitored IP addresses in seconds (default is 60 seconds)

Example :

```
./dhcp-stats -r dhcp.pcap -i eth0 -t 30 192.168.1.0/24 10.0.0.0/8
./dhcp-stats -r dhcp.pcap 172.16.1.0/28
./dhcp-stats -i eth0 172.16.1.0/28 10.1.1.1/24
./dhcp-stats -i  ./dhcp-stats -h
```

Literature

[1] AVOCADO, A. *DHCP Packet Analysis* [[online]]. 19.05.2020. [29.10.2023]. Available at: https://avocado89.medium.com/dhcp-packet-analysis-c84827e162f0.

[2] DROMS, R. *Dynamic Host Configuration Protocol* [RFC 2131]. RFC Editor, 1997. DOI: 10.17487/RFC2131. [29.10.2023]. Available at: https://www.rfc-editor.org/info/rfc2131.