ISA – Monitorování DHCP komunikace

Jakub, Sychra
xsychr06

November 20, 2023

Contents

Introduction

The goal of this project is to create a program to monitor DHCP traffic on the current device and monitor the utilization of specified devices. DHCP is a protocol built on a client/server model. DHCP servers assign network addresses and deliver their parameters to configured hosts. So the program has to correctly recognize appropriate DHCP messages and correctly act upon them.

Design and Implementation

Firstly, the arguments provided by the user in a terminal are checked.
Based upon these arguments, the program operates in either read or listening mode.

Arguments and ranges

Argument reading is done by using getopt. These arguments can be in any order as long as they don't simultaneously contain parameters for read and listen (-r and -i). After specifying the mode of the program, the program parses the user provided IP addresses and their masks.

IP addresses are converted to numerical values by separating each octet using the character '.' and are then manipulated using bitwise operations until a final numerical value is arranged. Due to this operation, the program can get any IP address and gets the subnet based on the combination of the provided IP and Mask.
Example: 192.168.0.1/8 $\longrightarrow$ 192.168.0.0/8

By using these numerical values, the process of comparing addresses and checking ranges is simplified, just as it helps by allowing the use of bitwise operations that can be done to the addresses themselves. One of these operations is the usage of the user provided mask. Using the mask, a certain amount of bits from the address are nulled to get the correct subnet, the highest and lowest addresses of the subnet and the maximum amount of allocatable hosts is determined with the subtraction of broadcast address and the network address. Due to the subtraction, this program is not designed to support mask /32. Using the mentioned data that was created using the bitwise operations, a global structure is then created containing all the specified IP ranges and their information.

Listening Mode

In the case of this mode, we have to specify the network interface on which the listening takes place. Before initiating the listening, the program checks whether the interface exists and is available. In this mode, a ncurses window[1] is also initiated to provide the user with up-to-date information about the prefixes. The ncurses window is only available in listening mode, and thus the implementation required the usage of a global value. The active listening is then initiated using the pcap_loop[2] method on the specified interface using the Packet Handler method.

Read Mode

In this mode, the user has to specify the file to be read. This access to the file is then verified, and afterwards the file is read using the pcap_loop method and the Packet Handler method.

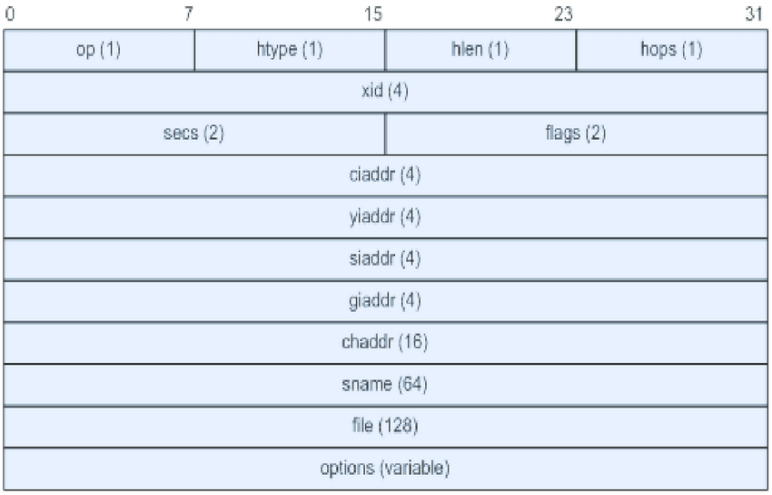

Figure 1: DHCP Packet Structure[3]

DHCP Packet Handler Method

This method processes packets, their ports and their types. The packet is verified whether it is an UDP packet and if it has the correct source port (67).
Afterwards if the packet is of the correct format, the data are loaded into a structure modeled after DHCP Packet(1).
In this structure, the Options part is checked for the correct Magic Cookie and is then cycled through until it reaches the end of the options or finds a DHCP Message.

Then the program checks the type of the DHCP Message, and proceeds if the message is of DHCP ACK type, in which case it takes the yiaddr part of the packet and verifies it to the global structure of ranges, and if it matches with any of the ranges, it is saved into those structures and appropriate data is incremented.

DHCP ACK is chosen as the sought-after message, as it's contained in DHCP communication relevant to the program.

Ending The Program

In the case that the program runs in read mode, the program ends after the reading of the file comes to an end, and in the case of listening mode, the program operates in a window and can be terminated with SIGINT (CTRL+C).

Manual

./dhcp-stats [-r <filename>] [-i <interface-name>] <ip-prefix> [<ip-prefix> [...]]

- -r <filename> pcap file to be read
- -i <interface-name> a network interface where DHCP monitoring will take place.
- <ip-prefix> IPv4 Address and its mask in the format x.x.x.x/y. User has to specify at least one prefix for the program to start. The mask is limited to the range of 1 to 31, thus excluding masks 0 and 32.

The arguments -r and -i can't be used at the same time.

References

[1] Ncurses programming howto. URL https://tldp.org/HOWTO/NCURSES-Programming-HOWTO/. Accessed on: 10.11.2023.

[2] pcap - packet capture library. https://www.tcpdump.org/manpages/pcap.3pcap.html. Accessed: [14.10.2023].

[3] Ralph Droms. Dynamic Host Configuration Protocol. RFC 2131, March 1997. URL https://www.rfc-editor.org/info/rfc2131.