ISA – Monitorování DHCP komunikace

Richard Kocián (xkocia19)

20. listopadu 2023

Obsah

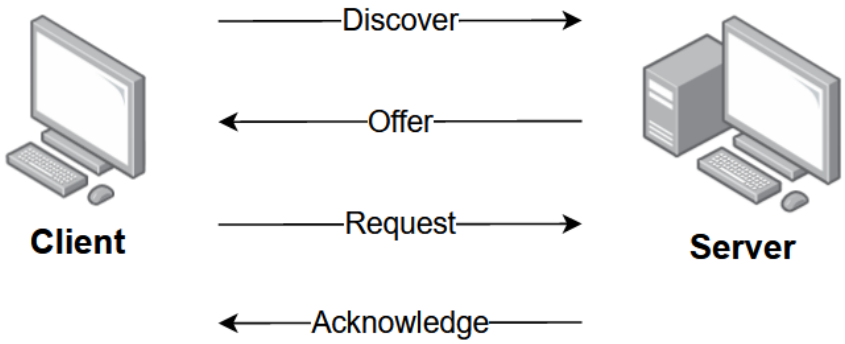
1 Uvedení do problematiky

1.1 DHCP (Dynamic Host Configuration Protocol)

Aby se zařízení mohlo připojit k síti, tak musí získat IP adresu. Protokol DHCP umožňuje počítačům a zařízením v síti dynamicky získávat IP adresy a další konfigurační síťové informace. Komunikace se skládá ze dvou prvků - klient a server.

1.2 DORA

Celý proces získání IP adresy se probíhá podle procesu DORA: Discover - Offer - Request - Acknowledge.



Obrázek 1: DORA proces [1]

1. Discover - klient vysílá broadcastovou zprávu na svoji lokální síť
2. Offer - když DHCP server zachytí Discover zprávu, tak danému zařízení zpět zašle nabídku (návrh, jakou IP adresu by klient mohl dostat přiřazenou), součástí Offer zprávy může být více nabídek
3. Request - klient příjme Offer zprávu (nabídku) a zašle serveru Request zprávu, kterou z nabídnutých IP adres si vybral
4. Acknowlede - server příjme Requst zprávu od klienta a klientovi danou IP adresu přiřadí -> zašle Acknowledge zprávu s potvrzením, že mu byla daná IP adresa přiřazena

2 Návrh aplikace

2.1 Vstupní parametry

Vstupem do aplikace budou parametry při spuštění. Konkrétně se bude jednat o rozhraní (interface), na kterém by se měly poslouchat DHCP packety, případně se může jednat o pcap soubor, ze kterého by program četl DHCP packety. Dalším vstupem bude jeden nebo více IPv4 prefixů sítě, který by měl program analyzovat.

2.2 Analýza IPv4 prefixů

Nejdříve by mělo dojít ke korektnímu zpracování IPv4 prefixů, které byly zadány jako argumenty aplikace. Z IPv4 prefixů bude potřeba zjistit, jaký je rozsah dané sítě. Tzn. zjistit, jaká je první volná IP adresa dané sítě a jaká je poslední volná IP adresa dané sítě, které můžeme klientovi přiřadit.

Musíme uvažovat, že při získání rozsahu dané sítě, který získáme maskováním, je první IP adresa rezervována jakožto síťová adresa dané podsítě a poslední IP adresa daného rozsahu je rezervována jakožto broadcastová adresa v rámci dané podsítě. Tyto adresy nelze klientovi přiřadit, proto by ani neměly být započítávány do zatížení daného síťového prefixu.

2.3 Zachytávání DHCP packetů

Poté bude potřeba, aby aplikace korektně zachytávala DHCP packety a korektně vyfiltrovala pouze packety zaslané od serveru nesoucí Acknowlede zprávu. Acknowlede zpráva bude jediná, která nás bude zajímat, jelikož až při ní je reálně IP adresa klientovi přiřazena.

Při přijetí Acknowledge zprávy bude potřeba ji korektně zpracovat - přečíst z ní, jakou IP adresu DHCP server klientovi přiřazuje. Následně se zkontroluje, zda daná IP adresa patří do některého z rozsahů vstupních IP prefixů.

2.4 Generování statistiky zatížení IP prefixu

Pokud získaná IP adresa z Acknowlede packetu do některého z vstupních IP prefixů nepatří, tak se nic nestane a pokračuje se čtením dalšího příchozího Acknowledge packetu.

Pokud ale daná IP adresu do některého IP prefixu patří (případně patří do více IP prefixů), tak se vytiskne statistika zatížení daného IP prefixu, kde počet alokovaných IP adres se zvýší o 1. Při překročení 50% zaplnění daného IP prefixu se do system logu zaloguje upozornění.

3 Popis implementace

3.1 Zpracování vstupních parametrů

Po spuštění aplikace se v metodě main v souboru main.cpp nejdříve zpracovají vstupní parametry aplikace skrz třídu ParamsParser.cpp.

Skrz standartní funkci getopt se kontroluje, zda je aplikace spuštěna pouze s povolenými vstupními parametry (pokud není, tak se vypíše nápověda a program skončí s exict code 1), v průběhu vykonávání této funkce se jednotlivé parametry naplní do lokálních proměnných dané třídy.

Následuje kontrola validity vstupních parametrů. Skrz regulární výraz se kontroluje, zda všechny zadané IP prefixy jsou validní. Pokud je zadán zároveň soubor a zároveň rozhraní, tak aplikace končí s chybou.

3.2 Analýza IPv4 prefixů

Každému zadanému IPv4 prefixu je vytvořen objekt třídy IP.cpp. Tyto objekty jsou následně uloženy do pole, které je uloženo v objektu třídy DHCPStats.cpp, což je hlavní třída celé aplikace, která zpracovává packety a generuje statistiku. V každém objektu IP.cpp jsou uloženy informace popisující tento prefix. Například obsahuje informace o první IP adrese daného rozsahu, o poslední IP adrese daného rozsahu, počet alokovatelných IP adres, funkci na zjištění, zda konkrétní IP adresa patří do daného rozsahu a aktuální obsazenost daného IP prefixu.

Rozsah daného IP prefixu se získá maskováním. Součástí IPv4 prefixu je IPv4 adresa a prefix (číslo od 0 - 32). Tento prefix určuje, že prvních x bitů adresy je neměnných. Bitovými operacemi tak lze zjistit první a poslední IP adresu a tak získat rozsah. Tento rozsah ještě musíme omezit, jelikož první a poslední IP adresa rozsahu je rezervována.

3.3 Zachytávání packetů a jejich filtrace na Acknowledge DHCP packety

Packety jsou zachytávány skrz standartní knihovnu pcap.h. Vše se odehrává ve tříde DHCPStats.cpp.

Před začátkem zachytávání se v případě zadaného souboru kontroluje, zda soubor existuje a využije se funkce pcap_open_offline(), v případě zadaného rozhraní se kontroluje, zda zadané rozhraní existuje, využívá se funkce pcap_open_live().

Následně skrz funkci pcap_next_ex() se získává další a další packet. Nejdříve proběhne kontrola, zda je získaný packet větší nebo roven než 236 Bytů, což je minimální velikost DHCP packetu [2]. Pokud je, tak se na získaný packet aplikuje ethernet hlavička z knihovny <net/ethernet.h>. Následuje kontrola, zda v ethernetové hlavičce je informace o tom, že se jedná o UDP packet (DHCP packety jsou zasílány skrz UDP protokol). Pokud se jedná o UDP packet, tak se kontroluje, zda zdrojový port je 67 (port DHCP serveru) a cílový port je 68 (port klienta) - standartně DHCP komunikuje skrz tyto porty.

Následuje aplikace dhcp struktury, která byla vytvořena na základě specifikace DHCP packetu [2]. Skrz tuto strukturu lze v options datech daného packetu zjistit, zda se jedná o Acknowledge paket a následně, jaká IP adresa byla DHCP serverem přiřazena.

3.4 Generování statistiky zatížení IP prefixů

Při zachycení IP adresy z Acknowledge packetu se projde pole IP prefixů a v případě, že daná IP adresa patří do rozsahu daného síťového prefixu, tak se vypíše statistika:

IP-Prefix Max-hosts Allocated addresses Utilization xxx.xxx.xxx.xxx/xx X X X

Při zaplnění prefixu z více jako 50%, nástroj informuje administrátora na zalogováním do systémového logu skrz funkci printToSysLog().

4 Základní informace o programu

4.1 Popis

Tento program umožňuje získat statistiku o vytížení zadaných síťových prefixů z pohledu množství alokovaných IP adres. Při zaplnění prefixu z více jako 50 %, nástroj o tomto informuje zalogováním do systémového logu.

Je možné jej spustit se zadaným pcap souborem, kdy daný soubor analyzuje, vypíše statistiku a následně skončí. Nebo je možné jej spustit na některém rozhraní, kdy program průběžně statistiku generuje při každém obdržení Acknowledge DHCP packetu, v takovém případě lze program ukončit ckrz CTRL+C.

5 Návod na použití

5.1 Překlad programu

Program lzre přeložit skrz: make

5.2 Synopsis

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

5.3 Vstupní parametry

-i Nastavení rozhraní, na kterém se budou poslouchat packety v případě nezadaného souboru.
-r Nastavení pcap souboru, ze kterého se budou číst packety v případě nezadaného rozhraní.
ip-prefix IPv4 síťové prefixy, ze kterých se má zpracovávat statistika. Formát: xxx.xxx.xxx.xxx/xx

6 Zdroje

Reference

[1] HOW COMPUTER GETs DHCP ADDRESS-DORA PROCESS. Online. Linkedin. 2023. Dostupné z: https://datatracker.ietf.org/doc/html/rfc2131. [cit. 2023-11-20].

[2] Dynamic Host Configuration Protocol. Online. Datatracker. 2023. Dostupné z: https://datatracker.ietf.org/doc/html/rfc2131. [cit. 2023-11-20].