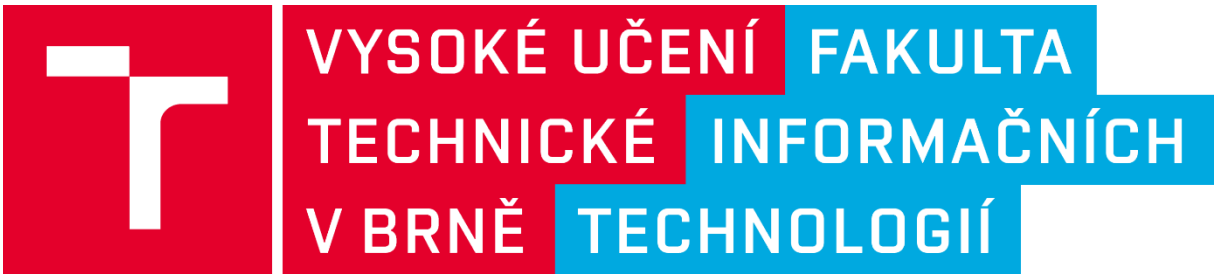

ISA – Sieťové aplikácie

Monitorovanie DHCP komunikácie

Adam Pap (xpapad11)

7.10. 2023

Obsah

..... 1
1 Úvod do problematiky 3
1.1 Teoretické východiská – DHCP 3
1.2 Skladba DHCP paketu 4
2 Popis implementácie 5
3 Informácie o programe 8
3.1 Spustenie programu 8
3.2 Testovanie programu 9
4 Zdroje 12

1 Úvod do problematiky

Zadaním tohto projektu bolo vytvorenie programu, ktorý bude vytvárať štatistiku o vyťažení sieťového prefixu z pohľadu množstva alokovaných IP adries. Program by mal vedieť spracovávať jak súbory s príponou .pcap tak aj monitorovať DHCP komunikáciu na používateľom zvolenom rozhraní. Následne by program mal vytvoriť štatistiku vyťaženia používateľom zvolených sieťových prefixov. Štatistika sa pri režime odpočúvania sieťového rozhrania periodicky aktualizuje. V prípade presiahnutia 50 % zaplnenia prefixu, program informuje používateľa na STDOUT a danú udalosť zaloguje prostredníctvom syslog serveru.

1.1 Teoretické východiská – DHCP

Táto kapitola bola inšpirovaná z [1] [2]

DHCP je aplikačný protokol, ktorý využíva protokol UDP. DHCP sa typicky využíva na auto konfiguráciu novo pripojených zariadení do siete. Toto novo pripojené zariadenie nevie aká je sieťová adresa danej siete ku ktorej sa pripojilo, ktorú IP adresu si má nastaviť, aká je dĺžka masky a pod. Toto zariadenie tiež nevie na ktorom zariadení (počítači) je spustený DHCP server, od ktorého by si mal vyžiadať vyššie spomenuté údaje. Jediné čo vie, je fakt že DHCP server (ak je nejaký v sieti vôbec nakonfigurovaný) počúva na porte 67.

Na základe tejto informácie vyšle správu cez UDP protokol, teda DHCP discover pre všetky zariadenia v danej sieti t.j. nastaví ako cieľovú adresu, adresu broadcastu lokálnej siete (255.255.255.255) a ako adresu zdroja nastaví (0.0.0.0). Táto správa obsahuje okrem iného aj náhodne vygenerovaný identifikátor.

Server následne reaguje na túto správu, správou DHCP offer, kde ponúka danému zariadeniu novú IP adresu. Na to aby táto správa prišla k danému zariadeniu DHCP server tiež nastaví ako cieľovú adresu, adresu broadcastu lokálnej siete. Správa tiež obsahuje ten istý identifikátor, aký bol v DHCP discover správe, IP adresu, životnosť IP adresy, default DNS servery, default router.

Následne, dané zariadenie reaguje správou DHCP request, ktorá požaduje pridelenie tejto IP adresy. Aj táto správa má za cieľovú IP adresu adresu bradcastu lokálnej siete a v tele má všetky parametre, ktoré prišli zariadeniu z DHCP offer správy.

Server teraz odpovie potvrdzovacou správou DHCP ACK. Táto správa ma tiež ako cieľovú adresu opäť adresu broadcastu. A po prijatí tejto potvrdzovacej správy zariadením, si nastaví ponúknutú IP adresu, masku a ďalšie parametre, ktoré mu boli ponúknuté.

1.2 Skladba DHCP paketu

DHCP paket pozostáva z :

op (1 bajt) – definuje typ správy (1 – BOOTREQUESTm 2 - BOOTREPLY)

htype (1 bajt) – definuje typ hardwarovej adresy

hlen (1 bajt) – definuje dĺžku hardwarovej adresy

hops (1 bajt) – klient nastavuje na 0, voliteľne používané tzv. „relay agents“ počas bootovania cez tzv. „relay agent“

xid (4 bajty) – definuje ID transakcie, je to v podstate náhodné číslo, ktoré si definuje klient, používané klientom a serverom na priradenie správ a odpovedí ktoré sa medzi nimi uskutočnili

secs (2 bajty) – vyplňované klientom, definuje čas (v sekundách) ktorý ubehol od začiatku procesu získavania sieťových parametrov

flags (2 bajty) – flags

ciaddr (4 bajty) – IP adresa klienta, toto pole je vyplnené len ak je klient v stave BOUND, RENEW, REBINDING a môže odpovedať ARP žiadostiam

yiaddr (4 bajty) – „vaša“ (klientska) IP adresa

siaddr (4 bajty) – IP adresa ďalšieho serveru pre použitie v „bootstrap“, táto aderesa je vrátená v správach DHCP offer, DHCP ACK

giaddr (4 bajty) – IP adresa tzv. „relay agent“ , použitá pre bootovaní cez tzv. „relay agent“

chaddr (16 bajtov) - klientska MAC adresa

sname (64 bajtov) – voliteľný názov hostiteľského serveru, vyplnené serverom ktorý posiela správu (DHCP offer, DHCP ACK)

file (128 bajtov) – názov bod súboru zvyčajne vyplnené serverom, ktorý posiela správy DHCP offer a DHCP ACK. Jedná prakticky o súbor ktorý by mal byť načítaný klientom

options (var) – voliteľné parametre

2 Popis implementácie

Program dhcp-stats.cpp sa skladá z hlavnej funkcie main(), skadiaľ program začína a z ďalších funkcií, ktoré dopĺňajú jeho funkcionalitu.

Program po spustení najprv spracuje užívateľom zadané parametre prostredníctvom `for` cyklu, kde kontroluje aj správnosť zadaných parametrov. Mimo iné kontroluje aj správnosť zadaných IP prefixov pomocou funkcie `is_validIP`. V prípade ak užívateľ nevie s akými parametrami môže program spustiť stačí ak ho spustí bez akýchkoľvek parametrov a na `STDOUT` sa mu vypíše pomocná krátka správa ako program spustiť, aké parametre podporuje a v akom poradí. Túto správu vypisuje program prostredníctvom `funkcie help_msg()`.

Následne program pokračuje nájdením vhodného rozhrania na odchytávanie paketov pomocou vstavanej funkcie z knižnice `libpcap`, `pcap_findalldevs`. Ak úspešne nájde takéto rozhranie otvorí ho pre odchytávanie paketov pomocou funkcie `pcap_open_live`. Potom sa nastaví filter na odchytávanie len určitých paketov (`pcap_compile`), v našom prípade nás zaujímajú len pakety DHCP, filter sa následne skompiluje a použije ďalej v programe. Filter sa nastavuje funkciou `pcap_setfilter`. Ďalej program pokračuje funkciou `pcap_loop`, čo je vlastne hlavná slučka pre odchyt paketov. Táto funkcia tiež volá funkciu `packetProcessing`, čo je vlastne funkcia spätného volania `(callback function)` pre každý odchytený paket kvôli jeho ďalšiemu spracovaniu.

To či užívateľ zadal spracovanie .pcap súboru alebo spracovanie paketov z rozhrania určuje premenná `file_or_interface`. Na základe hodnoty tejto premennej (0 – rozhranie, 1- .pcap súbor) sa určuje či sa zavolá funkcia `pcap_open_live` alebo `pcap_open_offline` a tiež to, či sa spustí terminálové rozhranie `ncurses` alebo sa výsledky len vypíšu na `STDOUT`.

Funkcia `packetProcessing` je spätným volaním, ktoré sa používa v `pcap_loop`, v ktorej dochádza k spracovaniu jednotlivých odchytených paketov. V prvom rade funkcia analyzuje a rozbaľuje paket. Ako prvé skontroluje či sa jedná o IP paket (tj. či hodnota `ether_type` v Ethernet hlavičke je rovná `ETHERTYPE_IP`). Potom sa skontroluje, či je IP protokol UDP (tj. či hodnota `protocol` v IP hlavičke je rovná `IPPROTO_UDP`). Následne sa skontroluje, či je zdrojový port UDP hlavičky 67, ktoré sú štandardné porty pre DHCP službu. Ak sú všetky tieto podmienky splnené, získa sa typ DHCP správy. Ak je typ DHCP správy 5 (tj. DHCP ACK), získa sa IP adresa pridelená klientovi (tj. pole `yiaddr`). Program ráta aj s možnosťou, že pole `Options` bude náhodne usporiadané, to znamená že `Option 53` (v ktorom sa nachádza typ DHCP správy) nemusí byť na začiatku poľa `Options`.

Následne sa iteruje cez jednotlivé užívateľom zadané IP prefixy, z ktorých sa vypočíta maximálny počet zariadení, ktoré sa do danej siete môžu pripojiť. Tento výpočet vykonáva funkcia `max_host_count()`. Ďalej sa zistí či daná yiaddr patrí do prefixu a ak áno tak sa vráti hodnota 1 z funkcie `allocated_address_count` ak nie vráti sa 0. Potom dochádza ku kontrole či sa IP adresa od užívateľa už nachádza v mape `stats` (štruktúra v hlavičkovom súbore dhcp-stats.hpp pre ukladanie štatistík, kde kľúčom je IP adresa s prefixom od užívateľa a hodnotou je štruktúra `subnet_stats`). Ak nie vytvorí sa nová inštancia v štruktúre

`subne_stats` (táto štruktúra je následne uložená v mape `stats`). Následne sa jednotlivé hodnoty štruktúry inicializujú a v prípade ak funkcia `allocated_address_count` vrátila 1, tak sa pripočíta +1 k alokovaným adresám daného prefixu a vypočíta sa percentuálny podiel využitia daného prefixu. Ak sa už IP adresa zadaná užívateľom už nachádza v mape `stats` tak sa len hodnoty aktualizujú a prepočíta sa percentuálny podiel využitia danej siete s daným prefixom.

A ak došlo k presiahnutiu 50% podielu využitia všetkých adries v danom prefixe užívateľ bude o tom upovedomený krátkym výpisom v terminály a tiež sa daná udalosť zaloguje prostredníctvom syslog serveru.

Avšak v prípade odchytávania paketov z rozhrania, program funguje ako konzolová aplikácia, to znamená že sa v reálnom čase v istých periódach aktualizuje množstvo alokovaných adries daných prefixov (ak daná adresa patrí do daného prefixu) a tiež percentuálny podiel využitia daného prefixu , toto je zabezpečené knižnicou `ncurses`. Na vynútené ukončenie programu (v prípade ak sa odpočúvajú paketuý zo sieťového rozhrania) stačí stlačiť skratku CTRL+c čo korektne ukončí program prostredníctvom funkcie `Signal_handler`. V prípade spracovania súborov sa toto nedeje, miesto toho sa po skončení analýzy vypisujú štatistiky na `STDOUT`. Ako posledné by som rád zmienil fakt, že názov súboru pre logovanie sa nazýva dhcp-stats.log.

`void help_msg()`

Metóda na vypísanie pomocnej správy.

`int is_validIP()`

Metóda skontroluje správnosť IP adries či náhodou neobsahujú iné než číselné znaky, či sa v jednom z oktetov nenachádza číslo väčšie ako 255 prípadne menšie ako 0 a v neposlednom rade či je uvedená aj maska za IP adresou v rozsahu od 0 do 32. Kontrola IP adresy je zabezpečená pomocou vstavanej funkcie `inet_pton`.

`int max_host_count()`

Metóda spočíta maximálny možný počet použitelných IP adries z daného IP prefixu. Extrahuje masku z danej IP adresy, ktorú zadal užívateľ a vráti 32 – hodnota masky)^2) -2. Na konci sa odčítava -2 preto lebo dve sú rezervované pre broadcast siete a jej identifikátor.

`int allocated_address_count()`

Metóda sa zaoberá zisťovaním či daná `yiaddr` patrí do daného prefixu a tým pádom prehlásiť, či daná adresa je alokovaná resp. priradená nejakému zariadeniu v sieti DHCP serverom. Toto sa deje prostredníctvom bitových súčinov, kedy sa vykonajú dva bitové súčiny. Prvý súčin sa vykoná medzi maskou IP prefixu zadanou používateľom a `yiaddr` a druhý bitový súčin sa vykoná medzi maskou IP prefixu zadanou používateľom a IP adresou

IP prefixu. Maska siete sa vypočíta ako bitový posun doprava na 32-bitovom čísle so všetkými bitmi nastavenými na 1.

Nakoniec sa skontroluje, či už bola adresa `yiaddr` priradená. Ak nie, pridá sa do zoznamu priradených adries a funkcia vráti 1. Inak vráti 0.

3 Informácie o programe

Jedná sa o program, ktorý vytvára štatistiku o využití sieťového prefixu z pohľadu množstva alokovaných IP adries.

Program pracuje v dvoch režimoch:

- režim spracovania .pcap súborov (`-r`)

  - výstupom tohto režimu je výpis tabuľky na `STDOUT`.

- režim odpočúvania DHCP komunikácie (`-i`)

  - výstupom tohto režimu je priebežne aktualizovaná tabuľka (prostredníctvom `ncurses`), ktorá používateľa informuje o percentuálnom podiele alokovaných prefixov.

Daná tabuľka má tieto stĺpce (platí pre oba režimy):

`IP-Prefix` - stĺpec zobrazujúci používateľom zadané ip-prefixy aj sa maskami.

`Max-hosts` - zobrazuje maximálny počet zariadení, ktoré sa do danej siete môžu pripojiť.

`Allocated addresses` - zobrazuje počet ip adries ktoré boli využité v rámci daného prefixu

`Utilization` - zobrazuje celklové využitie daného prefixu v percentách.

V prípade zaplnenia daného prefixu o viac ako 50% program informuje používateľa na `STDOUT` a danú udalosť zaloguje prostredníctvom syslog serveru.

Tiež by som rád upozornil že program na výstupe nezoraďuje prefixy podľa veľkosti, program pracuje len nad IPv4 adresami. Tunelovanie v rámci aplikácie nie je podporované. Program do štatistík počíta len IP adresy klientskych zariadení z poľa YIADDR.

Pri zadávaní IP prefixov, resp. sietí v ktorých sa má počítať využitie adries, sa od užívateľa očakáva znalosť aké prefixy sú validné a aké naopak nie, napr.: 192.168.1.1/24 je syntakticky validné avšak z pohľadu siete to nedáva zmysel.

3.1 Spustenie programu

Program vyžaduje aby systém na ktorom bude spustený mal nainštalované knižnice `libpcap` a `ncurses`. Tiež je potrebné aby v prípade zvolenia odchytávania paketov zo sieťového rozhrania bol program spustený príkazom `sudo`, bez tohto príkazu program nemá právo odchytávať pakety a preto sa skončí jeho vykonávanie. Tiež je vhodné zmieniť fakt, že program nepracuje v režime odpočúvania a spracovania DHCP packetov z rozhrania (-i) a spracovania súborov (-r) zároveň. Pracuje buďto to v režime odpočúvania a spracovania DHCP packetov z rozhrania (-i) alebo spracovania súborov (-r).

Prekladanie programu je pomocou priloženého Makefile súboru príkazom `make`. A spustenie programu je následné:

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

-r <filename> - štatistika bude vytvorená spracovaním .pcap súborov
-i <interface> - sieťové rozhranie na ktorom sa budú odchytávať pakety

<ip-prefix> - rozsah siete pre ktorú sa budú generovať štatistiky

Príklad spustenia:
./dhcp-stats -i eth0 192.168.1.0/24 192.168.0.0/22 172.16.32.0/24

./dhcp-stats -r pcap_file_name.pcap 192.168.0.0/22 192.168.1.0/24

3.2 Testovanie programu

Testovanie spracovania .pcap súboru:

./dhcp-stats -r pcaps/dhcp-homenetwork.pcap 192.168.0.0/22 192.168.1.0/24

IP-Prefix: 192.168.0.0/22, Max-hosts: 1022, Allocated addresses: 3, Utilization: 0.2935%

IP-Prefix: 192.168.1.0/24, Max-hosts: 254, Allocated addresses: 3, Utilization: 1.1811%

./dhcp-stats -r pcaps/dhcp-homenetwork.pcap 192.168.0.0/22 192.168.5.0/30

IP-Prefix: 192.168.0.0/22, Max-hosts: 1022, Allocated addresses: 3, Utilization: 0.2935%

IP-Prefix: 192.168.5.0/30, Max-hosts: 2, Allocated addresses: 0, Utilization: 0.0000%

- Tento súbor bol stiahnutý z nasledujúcej stránky:
  https://www.cloudshark.org/captures/19585c567c37

./dhcp-stats -r pcaps/DHCP.cap 192.168.0.0/22 172.16.32.0/24 192.168.1.0/24

IP-Prefix: 172.16.32.0/24, Max-hosts: 254, Allocated addresses: 0, Utilization: 0.0000%

IP-Prefix: 192.168.0.0/22, Max-hosts: 1022, Allocated addresses: 1, Utilization: 0.0978%

IP-Prefix: 192.168.1.0/24, Max-hosts: 254, Allocated addresses: 0, Utilization: 0.0000%

- Tento súbor bol stiahnutý z nasledujúcej stránky:
  https://packetlife.net/captures/protocol/bootp/

Testovanie odchytávania DHCP paketov zo sieťového rozhrania:

- Upozornenie, v tomto prípade program nešiel otestovať na serveri `Merlin` nakoľko ako študent nemám právo spustiť program v režime `sudo`, preto som program testoval na svojom PC (WSL). Sieťovú prevádzku som simuloval `python` skriptom za použitia knižnice `scapy`.

sudo ./dhcp-stats -i eth0 192.168.1.0/24 172.16.32.0/24 192.168.5.0/30 192.168.0.0/22

IP-Prefix	Max-hosts	Allocated addresses	Utilization
172.16.32.0/24	254	0	0.00%
192.168.0.0/22	1022	0	0.00%
192.168.1.0/24	254	0	0.00%
192.168.5.0/30	2	2	100.00%

prefix 192.168.5.0/30 exceeded 50% of allocations

- Najprv som poslal 2 pakety s yiaddr od 192.168.5.1 – 192.168.5.2, je vidieť že prefix ma už zaplnenie 100%, čo vyplýva z jeho max hosts stĺpca. A v priečinku `var/logs`, v súbore `syslog` sa objavil nový záznam: `Oct 7 21:01:27 LAPTOP-N5BFSQEL dhcp-stats[521]: prefix 192.168.5.0/30 exceeded 50% of allocations.`

IP-Prefix	Max-hosts	Allocated addresses	Utilization
172.16.32.0/24	254	0	0.0000%
192.168.0.0/22	1022	20	1.9600%
192.168.1.0/24	254	20	7.8740%
192.168.5.0/30	2	2	100.0000%

prefix 192.168.5.0/30 exceeded 50% of allocations

- Následne som poslal 20 paketov s yiaddr od 192.168.1.1 – 192.168.1.20, v tomto prípade sa budú IP prefixy prekrývať.

IP-Prefix	Max-hosts	Allocated addresses	Utilization
172.16.32.0/24	254	0	0.0000%
192.168.0.0/22	1022	25	2.4462%
192.168.1.0/24	254	20	7.8740%
192.168.5.0/30	2	2	100.0000%

prefix 192.168.5.0/30 exceeded 50% of allocations

- Následne som poslal 5 paketov s yiaddr od 192.168.3.1 – 192.168.3.5, v tomto prípade sa IP adresy započítajú len do IP prefixu 192.168.0.0/22.

IP-Prefix	Max-hosts	Allocated addresses	Utilization
172.16.32.0/24	254	0	0.0000%
192.168.0.0/22	1022	25	2.4462%
192.168.1.0/24	254	20	7.8740%
192.168.5.0/30	2	2	100.0000%

prefix 192.168.5.0/30 exceeded 50% of allocations

- Následne som poslal opäť 20 paketov s yiaddr od 192.168.1.1 – 192.168.1.20, ako je vidieť na výpise, nič sa nezmenilo nakoľko dané adresy už boli raz započítané do štatistík.

IP-Prefix	Max-hosts	Allocated addresses	Utilization
172.16.32.0/24	254	20	7.8740%
192.168.0.0/22	1022	25	2.4462%
192.168.1.0/24	254	20	7.8740%
192.168.5.0/30	2	2	100.0000%

prefix 192.168.5.0/30 exceeded 50% of allocations

- Následne som poslal opäť 20 paketov s yiaddr od 172.16.32.1 – 192.16.32.20, ako je vidieť adresy sa pričítali tam kam mali.

IP-Prefix	Max-hosts	Allocated addresses	Utilization
172.16.32.0/24	254	20	7.8740%
192.168.0.0/22	1022	25	2.4462%
192.168.1.0/24	254	20	7.8740%
192.168.5.0/30	2	2	100.0000%

prefix 192.168.5.0/30 exceeded 50% of allocations

- Následne som poslal opäť 20 paketov s yiaddr od 192.168.1.1 – 192.168.1.20, a ako je vidieť adresy sa nepričítali nakoľko tieto IP adresy už boli predtým pričítané.

4 Zdroje

Institute of Computer Science UPJS. 6. Prednáška – Sieťová vrstva 1 [online]. Košice: Institute of Computer Science UPJS. [cit. 07.10.2023]. Dostupné z: https://siete.ics.upjs.sk/prednaska-6/

Network Working Group R. Droms. RFC 2131 - Dynamic Host Configuration Protocol [online]. March 1997. [cit. 07.10.2023]. Dostupné z: https://datatracker.ietf.org/doc/html/rfc2131

Fakulta informačních technologií VUT v Brně. STUDIS ISA/Detail Předmětu/Zadnání [online]. Brno: Fakulta informačních technologií VUT. [cit. 07.10.2023]. Dostupné z: https://www.vut.cz/studis/student.phtml?sn=zadani_detail&apid=268266&zid=54265

Converting subnet mask prefix with C – Stack Overflow. Stack Overflow – Where Developers Learn, Share, & Build Careers [online]. [cit. 07.10.2023]. Dostupné z: https://stackoverflow.com/questions/16072967/converting-subnet-mask -prefix-with-c

The Sniffer's Guide to Raw Traffic (a libpcap tutorial). [online]. [cit. 07.10.2023]. Dostupné z: http://yuba.stanford.edu/~casado/pcap/section1.html

Writing manual pages. [online]. 2019-01-06 08:48. [cit. 14.10.2023]. Dostupné z: https://liw.fi/manpages/

NCURSES Programming HOWTO. [online]. v1.9, 2005-06-20. [cit. 14.10.2023]. Dostupné z: https://tldp.org/HOWTO/NCURSES-Programming-HOWTO/index.html