Vysoké učení technické v Brně
Fakulta informačních technologií

Síťové aplikace a správa sítí – Projekt

Monitorování DHCP komunikace

17. novembra 2023 Marián Tarageľ (xtarag01)

Obsah

1 Úvod

Tento manuál stručne zhrnie základný popis programu `dhcp-stats`, teoretické základy DHCP komunikácie, implementačné riešenie projektu a limity súčasnej implementácie.

2 Popis programu

Program `dhcp-stats` je jednoduchá sieťová aplikácia, ktorá monitoruje DHCP komunikáciu a priebežne zobrazuje vyťaženie IP prefixov. Pokiaľ zaplnenie IP prefixu presiahne 50%, tak program o tom informuje administrátora pomocou štandardnej služby syslog.

Program pracuje vo dvoch režimoch a to „online“ (prepínač `-i`) alebo „offline“ (prepínač `-r`). V „online“ monitoruje komunikáciu priamo na sieťovom rozhraní. Druhou možnosťou je použitie pcap súboru z ktoré program prečíta zachytenú DHCP komunikáciu.

2.1 Syntax spustenia

Program `dhcp-stats` sa spúšťa z príkazového riadku terminálu nasledujúcim príkazom:

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

- `-r` – názov pcap súboru z ktorého sa bude čítať DHCP komunikácia
- `-i` – názov sieťového rozhrania z ktorého sa budú odchytávať pakety
- `ip-prefix` – sieťový prefix pre ktorý sa má generovať štatistika

Prepínače `-r` a `-i` nie je možné kombinovať, ale vždy musí byť zadaný aspoň jeden z nich. IP prefixov môže byť aj viac a môžu sa aj prekrývať. Očakávný fromát IP prefixu je x.x.x.x/y, kde x.x.x.x je platná IPv4 adresa a y je dĺžka sieťového prefixu (rozsah 0 - 32). Ak užívateľ zadá nie úplne korektný IP prefix, napríklad 192.168.1.15/24, tak sa IP adresa vymaskuje podľa dĺžky prefixu a ďalej sa používa sieťová IP adresa 192.168.1.0/24 ale vo výpise sa zobrazí pôvodná adresa 192.168.1.15/24. Argumenty môžu byť v ľubovoľnom poradí.

Okrem vyššie uvedených prepínačov, je možné pomocou `-h` alebo `--help` vypísať nápovedu. Argument `--version` vypíše informácie o aktuálne používanej verzii programu.

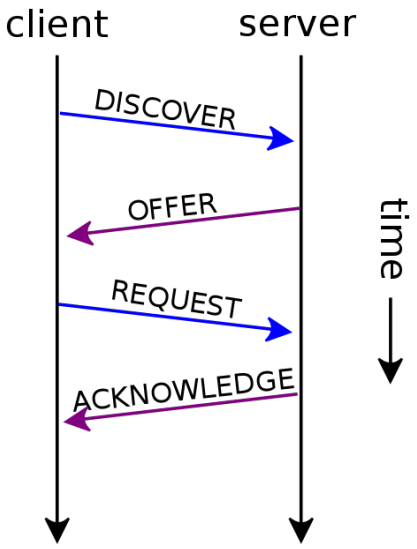
2.2 Príklad spustenia

```
$ ./dhcp-stats -i eth0 192.168.1.0/24 172.16.32.0/24 192.168.0.0/22
IP-Prefix Max-hosts Allocated addresses Utilization
192.168.0.0/22 1022 123 12.04%
192.168.1.0/24 254 123 48.43%
172.16.32.0/24 254 15 5.9%
```

3 Protokol DHCP

Protokol DHCP (Dynamic Host Configuration Protocol) je sieťový protokol, ktorý umožňuje odovzdať konfiguračné nastavenia klientovi v rámci TCP/IP siete. DHCP umožňuje automatické prideľovanie IP adries pre nové zariadenia v sieti a nastavenie dodatočných konfiguračných nastavení.[3]

Na obrázku 1 je znázornený typický príklad DHCP komunikácie. Ako prvú posiela klient správu DHCP Discover, ktorou oznámy serveru, že do siete prišlo nové zariadenie, ktoré chce novú IP adresu. Server odpovedá správou typu DHCP Offer v ktorej ponúkne klientovy IP adresu. Klient pomoucou správy DHCP Request požiada server o IP adresu uvedenú v DHCP Offer a automaticky zamietne všetky ostatné ponuky. Server správou DHCP Ack potvrdí pridelenie IP adresy.



Obr. 1: Ukážka DHCP komunikácie. [6]

3.1 Formát DHCP správy

V tabuľke 1 je znázornený formát DHCP správy. Jednotlivé položky sú bližšie špecifikované v tabuľke 2. Číslo v zátvorke vyjadruje veľkosť poľa v bajtoch.

op (1)	htype (1)	hlen (1)	hops (1)
xid (4)			
secs (2)		flags (2)	
ciaddr (4)			
yiaddr (4)			
siaddr (4)			
giaddr (4)			
chaddr (16)			
sname (64)			
file (128)			
options (variable)			

Tabuľka 1: Formát DHCP správy [3].

Pole	Veľkosť	Popis
op	1 B	Typ správy
htype	1 B	Typ fyzickej adresy
hlen	1 B	Dĺžka fyzickej adresy
hops	1 B	Počet skokov, pre DHCP relay
xid	4 B	ID tranzakcie
secs	2 B	Počet sekúnd od získania alebo obnovy IP adresy
flags	2 B	Broadcast alebo unicast
ciaddr	4 B	IP adresa klienta
yiaddr	4 B	IP adresa pridelená klientovi
siaddr	4 B	IP adresa servera
giaddr	4 B	IP adresa relay agenta
chaddr	16 B	Fyzická adresa klienta
sname	64 B	Meno servera
file	128 B	Názov boot súboru
options	var	Ďalšie parametre

Tabuľka 2: Popis položiek DHCP správy [3, 5].

3.2 Typy DHCP správ

Protokol DHCP definuje typy správ, ktoré si medzi sebou vymieňajú klient a server. Medzi štyri základné patrí DHCP Discover, DHCP Offer, DHCP Request a DHCP Ack.

- **DHCP DISCOVER** – Posiela ju klient na broadcast, aby zistil dostupné DHCP servery.
- **DHCP OFFER** – Odpoveď servera na DHCP DISCOVER s ponukou novej IP adresy.
- **DHCP REQUEST** – Správa klienta na server, ktorá buď žiada o ponúknutú IP adresu, alebo potvrdzuje správnosť už pridelenej IP adresy, alebo žiada o predĺženia času na používanie IP adresy.
- **DHCP ACK** – Správa od servera ku klientovi, ktorá potvrdzuje pridelenie IP adresy. [3]

4 Návrh aplikácie

Program `dhcp-stats` bol napísaný v jazyku C. Implementovaný je v dvoch súboroch a to `dhcp--stats.c` a `dhcp-stats.h`. Štruktúrne je delený do viacerých funkcií, ktoré vykonávajú jednoduchšie úlohy.

Základnou funkciou je `main()`, ktorá volá ostatné funkcie a zabezpečuje korektné zotavenie z chybových stavov. Na začiatku sa spracujú argumenty príkazového riadku, potom sa pomocou funkcie `open_pcap()` nadviaže spojenie na sieťové rozhranie alebo sa otvorí pcap súbor. Následne sa aplikuje filter, aby sa prijímali iba UDP pakety z portov 67 alebo 68. Potom program čaká na pakety v nekonečnej slučke. Ak príde DHCP paket s novo alokovanú IP adresu, aktualizuje sa výpis štatistík.

5 Implementácia

Pri implementácii som sa používal návod na programovanie v libpcap [2], ncourses [4], syslog [1] a linuxové manuálové stránky.

Spracovanie argumentov príkazového riadku je implementované ručne a to dvojfázovým priechodom. Pri prvom priechode sa kontroluje prítomnosť prepínačov `-h`, `--help` alebo `--version`. Následne sa spracujú všetky argumenty, ktoré sa uložia do štruktúry `cmd_options_t`.

Vo funkcii `read_packets()` sa v cykle typu while čaká na príchod paketov, ktoré sú analyzované. Extrahuje sa z nich DHCP hlavička (ak ju obsahujú) a určí sa typ DHCP správy. Ak ide o DHCP Ack, tak sa najskôr skontroluje či sa nejedná o sieťovú alebo broadcastovú IP adresu, lebo tie nemôžu byť pridelené klientovi. Potom sa ešte overí vo funkcii `is_ipaddr_in_list()`, či program už túto IP adresu nezapočítal, aby sa zabránilo duplicitnému pripočítavania adries. Ak ju nepozná, tak si ju pridá do zoznamu IP adries, ktoré už spracoval a aktualizuje štatistiky. Ak zaplnenie IP prefixu presiahne 50%, tak sa pomocou knižnice `syslog.h`, táto udalosť zapíše do systémového logu a zároveň sa vypíše do terminála. Ak viac prefixov prekročí túto hranicu, tak sa v každý zaloguje v samostatnej správe do `syslogu` ale v termináli sa vždy bude prepisovať iba jeden riadok.

Štatistiky sú zapisované do terminálového okna vytvoreného pomocou knižnice `ncurses.h` aj pri variante zachytávania paketov zo sieťového rozhrania aj pri čítaní paketov z pcap súboru. Toto okno je vždy nutné uzavrieť pomocou príkazu `Ctrl + c`, aj keď bol prečítaný celý pcap súbor. Ak by sa v tomto momente vystúpilo z cyklu a ukončil by sa program, tak by sa zavrelo aj terminálové okno a štatistiky by neboli viditeľné dlhšiu dobu.

Ukončenie programu je riešené zaslaním signálu `SIGINT` alebo stlačením klávesovej kombinácie `Ctrl + c`. To vyvolá spustenie obslužnej rutiny, funkcia `signal_handler()`. V nej sa zavolá funkcia `pcap_breakloop()`, ktorá preruší `pcap_next_ex()` a následne sa nastaví globálna premenná `end_loop` na `TRUE` aby sa zastavila nekonečná slučka. Potom program uvoľní alokované zdroje, zavrie terminálové okno a ukončí program.

5.1 Limity implementácie

V súčasnej implementácii projektu, program `dhcp-stats` nepodporuje adresy typu IPv6 a správy typu DHCP RELEASE a DHCP DECLINE. Taktiež nie je podporované sledovanie vypršania platnosti IP adresy (lease time) a ani DHCP pakety, ktoré obsahujú option overload, alebo boli poslané z virtuálnej siete (VLAN). Pri prepínači `-r` je podporovaný maximálne jeden pcap súbor.

Literatúra

[1] ALLMAN, E.: Syslog Example. [online], [cit. 2023-11-11]. Dostupné z: https://www.gnu.org/software/libc/manual/html_node/Syslog-Example.html

[2] CARSTENS, T.: Programming with pcap. [online], 2002, [cit. 2023-11-11]. Dostupné z: https://www.tcpdump.org/pcap.html

[3] DROMS, R.: Dynamic Host Configuration Protocol. RFC 2131, Marec 1997, doi:10.17487/RFC2131. Dostupné z: https://www.rfc-editor.org/info/rfc2131

[4] PADALA, P.: NCURSES Programming HOWTO. [online], 2005, [cit. 2023-11-11]. Dostupné z: https://tldp.org/HOWTO/NCURSES-Programming-HOWTO/

[5] VESELÝ, V.: Síťová vrstva. [IPK lecture], 2023, [cit. 2023-11-11].

[6] WIKIMEDIA: Dynamic Host Configuration Protocol. [online], 2023, [cit. 2023-11-11]. Dostupné z: https://en.wikipedia.org/wiki/Dynamic_Host_Configuration_Protocol#/media/File:DHCP_session.svg