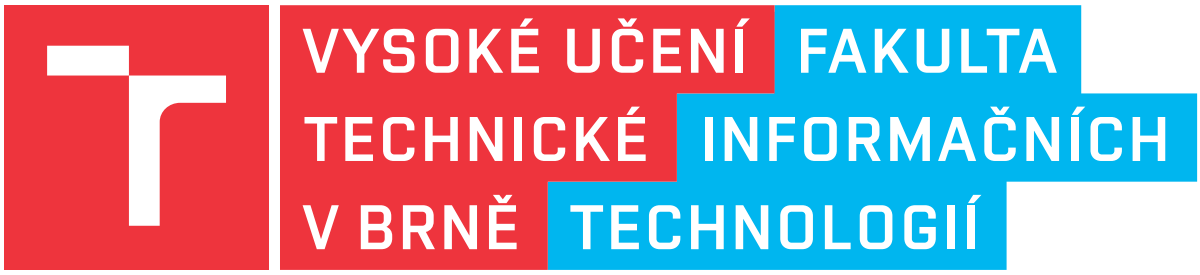

Síťové aplikace a správa sítí – projekt

Monitorování DHCP komunikace

Manuál

9. listopadu 2023

Matúš Vráblik (xvrabl05)

Obsah

1 Úvod

Cieľom projektu je monitorovať vyťaženie adresného priestoru. V praxi sa používa pre tieto účely výpis z logu DHCP servera. Tento projekt sa zameriava na prípad keď nie je možné získať potrebné logy z DHCP servera a riešim to monitorovaním DHCP komunikácie.

2 DHCP

Protocol DHCP[1][1] sa skladá zo správ DHCPDISCOVER, DHCPOFFER, DHCPREQUEST, DHCPACK, DHCPNAK, DHCPDECLINE, DHCPRELEASE, DHCPINFORM a podla štandardu je na UDP portoch 67(server) a 68(klient). Zo správ ma ale zaujímajú len správy DHCPACK a DHCPRELEASE, ktoré mi postačujú pre tento projekt. Z nich viem zistit ktorá adresa bola poskytnutá alebo uvoľnená.

Správa DHCPACK slúži na potvrdenie priradenia adresy klientovi a teda posiela ju server klientovi. Správa DHCPRELEASE slúží zase na uvoľnenie adresy a posiela ju klient serveru. Keďže ide o nepovinnú správu musím vedieť vyradiť adresu aj na základe *lease time* 1. Podľa RFC 2131[4][2] musia tieto správy obsahovať hodnoty, z ktorých som vybral len tie ktoré „musia“ alebo „nesmú“ byť obsiahnuté.

Option	**DHCPACK**	**DHCPRELEASE**
Requested IP address	-	-
IP address lease time	+	-
DHCP message type	„DHCPACK“	„DHCPRELEASE“
Parameter request list	-	-
Vendor class identifier	?	-
Server identifier	+	+
Maximum message size	-	-
Site-specific	?	-
All-other	?	-

’+’ = musí obsahovať, ’-’ = nesmie obsahovať, ’?’ = môže obsahovať

Tabulka 1: Tabulka hodnôt v poli „options“.

2.1 Doba vypožičania - *Lease time*

Táto možnosť určuje dobu po ktorú je daná IP adresa pridelená klientovi. Po uplynutí tejto doby je adresa znova voľná. Pre predĺženie doby vypožičania si klient žiada o aktuálne pridelenú adresu ešte pred vypršaním jej platnosti.

3 Implementačné detaily

Program monitoruje iba IPv4,UDP,DHCP komunikáciu. UDP komunikácia musí byť na portoch 67 a 68, v inej kombinácii ako napríklad 67 a 67 nemá zmysel a preto takéto packety zahadzujem. Program obsahuje CLI manuál[3] `dhcp-stats.1`

[1] Dynamic Host Configuration Protocol https://www.rfc-editor.org/rfc/rfc2131.html
[2] DHCPACK, DHCPRELEASE

3.1 Štruktúra kódu

3.1.1 Rozšírenia

Riešenie obsahuje 2 časti ktoré možu byť brané ako rozšírenia.

1. Lease time - Aktualizujem túto dobu pri DHCPACK správe so zhodnou IP adresou a uvolním adresu pri vypršaní.
2. DHCPRELEASE - uvolním adresu pri tejto správe.

3.1.2 Funkcie

- **main()**
  1. Parsuje argumenty pomocou `getopt`.
  2. Zvolý pracovný mód podľa vstupných argumentov a vytvorý premennú `pcap_t* handle`pomocou funkcií `pcap_open_live()` alebo `pcap_open_offline()` podľa zvoleného módu.
  3. Vytvorý globálnu premennú vlastného typu `p_map` v ktorej vytvorý N záznamov, kde N je počet zadaných prefixov pri spustení.
  4. Inicializuje prostredie pre `ncurses` knižnicu[2].
  5. Spracuje packety pomocou `pcap_loop()` s nazvom funkcie `handle_pcap()` ako parameter pre callback.
  6. Ukončí prostredie pre `ncurses` knižnicu.
- **handle_pcap()**
  1. Skontroluje eternetovú hlavičku paketu pre IPv4.
  2. Skontroluje ip hlavičku pre UDP protokol.
  3. Overí v UDP hlavičke správnosť portov.
  4. Vytriedi DHCP pakety podľa tabuľky 1.
  5. Zavolá funkciu `check_lease_time()` pre rozšírenie 1.
  6. Vytvorí premennú `dhcp_mon` vlastného typu `dhcp_monitor`.
  7. Aktualizuje globálnu premennú typu `p_map` pomocou funkcie `update_global_map(dhcp_mon)`.
  8. Aktualizuje zobrazené okno z knižnice `ncurses` funkciou `update_win()`.
- **update_global_map()**
  Pridanie/odobranie adresy z rozsahu je zabezpecené boolovskou hodnotou `rm` vo vstupnej premennej do tejto funkcie vlastného typu `dhcp_monitor`. Okrem aktualizovania globálnej mapy počíta utilizáciu prefixov a v prípade utilizácie vyššej ako 50% vypíše hlášku pomocou `syslog()`. Pre zaradenie jednotlivých packetov k správnemu rozsahu sa vytvorí v tejto funkcii mapa masiek ktore sa aplikujú na IP z argumentov a na IP v packete bitovou AND operáciou. Zhoda znamená adresa z paketu patrí do rozsahu prefixu.
- **check_lease_time()**
  Porovná čas každej priradenej ip adresy adresy s aktuálnym časom, ktorý sa aktualizuje každým prečítaným paketom. V prípade rozdielu väčšieho ako doba výpožičky sa priradená adresa vymazáva z mapy štatistík.

3.1.3 Vlastné typy

- p_map - mapa kde prefix s ip je klúčom do mapy a dvojica maximálneho počtu alokovaných adries a `dhcp_map` je hodnotou.
- dhcp_map - mapa kde ip adresa z paketu je kľúčom a `dhcp_monitor` je hodnotou
- dhcp - štruktúra pre dhcp paket podla rfc 2131 aj s „magic packet“
- dhcp_monitor - štruktúra pre aktualizáciu štatistík a kontrolu doby výpožičky.

4 Použitie

```
./dhcp-stats (-r <filename>|-i <interface>) <ip-prefix> [<ip-prefix>[...]] [-s]
```

- $-r < filename >$
  Vytvorí štatistiku zo súboru
- $-i < interface >$
  Vytvorí štatistiku zo vstupu z rozhrania, nutno ukončiť manuálne pomocou CTRL^C
- $< ip - prefix >$
  IP s prefixom v tvare N.N.N.N/X kde N je cislo medzi 0-255 a X je cislo medzi 0-30 pretože hodnota 31 pre 32 bitovu adresu by znamenala 0 volných adries a 32 by znamenalo -2 volné adresy.
- $[-s]$
  Prepínač krokového módu. Pri stlačení klávesy ktorá zaznamená viac ako 1 znak sa vykoná viac ako 1 krok programu.

Reference

[1] Dynamic host configuration protocol. [online], [rev. 2023-09-5], [cit. 2023-09-11].
URL `https://en.wikipedia.org/wiki/Dynamic_Host_Configuration_Protocol`

[2] *Ncurses*. [online], [rev. 2023-09-5], [cit. 2023-09-11].
URL `https://www.gnu.org/software/libc/manual/html_node/Syslog-Example.html`

[3] *Manpages*. [online], [rev. 2023-09-5], [cit. 2023-09-11].
URL `https://liw.fi/manpages/`

[4] *RFC 2131*. [online], [rev. 2023-09-5], [cit. 2023-09-11].
URL `https://www.rfc-editor.org/rfc/rfc2131.html`