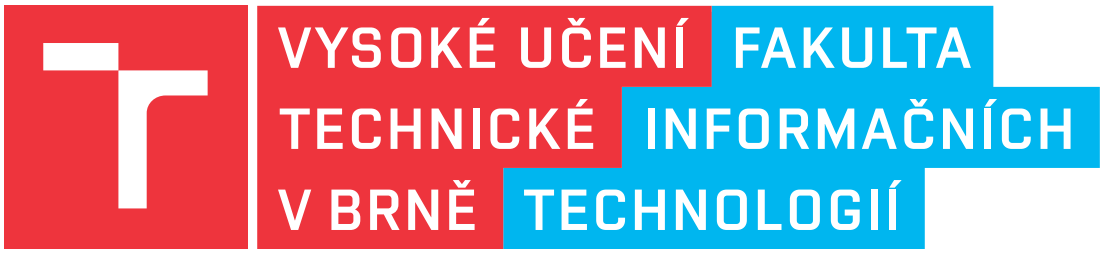

Síťové aplikace a správa sítí

Monitorování DHCP komunikace

13. listopadu 2023 Adrián Matušík (xmatus35)

Obsah

1 Úvod

Cieľom projektu bolo vytvoriť program, který umožní získat štatistiku o vyťažení sieťového prefixu z pohľadu množstva alokovaných IP adries. Pri zaplnení prefixu z viac ako 50%, nástroj informuje administrátora na štandardný výstup a zalogovaním skrz syslog server.

Tento problém sa v praxi rieši typicky pomocou parsingu pridelených adries z logu DHCP serveru, prípadne túto informáciu môže niekedy poskytnúť priamo DHCP server. Cieľom projektu je vyriešiť situáciu, keď DHCP server túto možnosť nepodporuje a pre získanie daných štatistík je možné monitorovať DHCP komunikáciu.

1.1 Monitorovanie DHCP komunikácie

Monitorovanie DHCP komunikácie znamená sledovanie a analyzovanie komunikácie medzi DHCP serverom a klientmi v sieti. DHCP (Dynamic Host Configuration Protocol), je sieťový protokol, ktorý umožňuje pridelenie IP adries a konfiguračných informácií zariadeniam v sieti automaticky.

Tu sú niektoré kroky, ktoré môže monitorovanie DHCP komunikácie zahrnovať:

- **Zachytávanie paketov** - používa sa sieťový nástroj na zachytávanie paketov, ako napríklad Wireshark alebo tcpdump, na odchytávanie DHCP paketov v sieti.
- **Analýza paketov** - pakety sú analyzované na identifikáciu DHCP paketov. DHCP komunikácia zahŕňa rôzne typy paketov ako sú DISCOVER, OFFER, REQUEST, a ACKNOWLEDGE. Analyzované sú aj konkrétne informácie v týchto paketoch, ako sú pridelené IP adresy, časové značky, a konfiguračné možnosti.
- **Identifikácia problémov** - monitorovanie DHCP komunikácie môže pomôcť identifikovať problémy v sieti, ako sú konflikty IP adries, neúspešné pokusy o pridelenie adries, alebo nečakané oneskorenie pri odpovedi od DHCP servera.
- **Štatistiky a sledovanie využitia** - zaznamenávanie a sledovanie štatistík môže poskytnúť informácie o tom, koľko IP adries je pridelených, aké sú dostupné rozsahy adries, a aké sú časy odpovedí od DHCP servera.
- **Záznamy a logy** - ukladanie záznamov o DHCP komunikácii môže byť užitočné pre neskoršiu analýzu a audit. Záznamy môžu obsahovať informácie o každej pridelenej IP a identifikovať nepravidelnosti alebo opakujúce sa problémy.
- **Alarmy a upozornenia** - nástroje na monitorovanie môžu byť nastavené na generovanie upozornení alebo alarmov v prípade zistenia nepravidelností alebo neštandardného správania sa v sieti.

Pre účely tohto projektu implementujem zachytávanie a analýzu paketov a štatistiku využitia. Pakety sa získavajú z .pcap súboru alebo z rozhrania, na ktorom program počúva. Analyzujú sa IPv4 pakety, bežiace nad UDP protokolom s portom serveru 67 a s portom klienta 68, a kontroluje sa či sa jedná o platné DHCP ACK(ACKNOWLEDGE) pakety, čo sa kontroluje v poli *options* v DHCP pakete. Na výstup programu sa vracia štatistika vyťaženia jednotlivých adresných priestorov.

Celkovo je monitorovanie DHCP komunikácie dôležité pre správu a bezpečnosť siete. Pomáha administrátorom sledovať využitie IP adries, identifikovať problémy v sieti, a zabezpečiť efektívne pridelenie IP adries klientom v sieti.

2 Implementácia

Program je navrhnutý v jazyku C++.

- Najskôr kontroluje vstupné argumenty, podľa ktorých sa prepne do módu na čítanie zo súboru alebo z rozhrania.
- Zo zadaných prefixov sa vypočíta maximálny počet voľných adries pre daný prefix.
- Pokračuje čítaním paketov z .pcap súboru alebo z rozhrania.
- Z paketov sa vyberú len IPv4 pakety, ktoré bežia nad UDP protokolom s portom serveru 67 a s portom klienta 68 a zisťuje sa, či sa jedná o platný DHCP ACK paket, ktorý má v poli *options* s klúčom *53* hodnotu *„DHCP_ACK“* a v poli *options* musí obsahovať *IP address lease time* a *Server identifier* a nesmie obsahovať *Requested IP address*, *Parameter request list*, *Client-identifier* a *Maximum DHCP message size*.
- Z platných paketov ďalej zisťuje či adresa patrí do rozsahu zadaných prefixov. IP adresy a masky siete sa prevedú na bitovú reprezentáciu a pomocou bitovej operácie AND medzi IP adresou paketu a maskou a IP adresou prefixu a maskou sa zistí, či daná IP adresa patrí do daného adresného rozsahu.
- V prípade že adresa patrí pod daný prefix, tak sa započíta do alokovaných adries pre daný prefix.
- Z počtu voľných a alokovaných adries jednotlivých prefixov sa vypočítava využitie adresného rozsahu.
- Všetky tieto zmienené údaje ako sú prefix, počet voľných adries, počet alokovaných adries a využitie adresného rozsahu sa vypisujú do tabuľky pomocou knižnice *ncurses*.
- Tento program rieši celkové využitie adresného priestoru za čas behu programu, uvoľnené adresy neodpočítava, ani ich nerieši.

3 Použitie

Program musí podporovať nasledujúcu syntax pre spustenie:

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

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

-r <filename> - štatistika bude vytvorená z pcap súborov
-i <interface> - rozhranie, na ktorom môže program počúvať
<ip-prefix> - rozsah siete pre ktorý sa bude generovať štatistika

Program očakáva na vstupe jeden z povinných parametrov -r, alebo -i. Program nepodporuje oba parametre súčastne, avšak v oboch prípadoch očakáva minimálne jeden <ip-prefix>.

Pre prípad čítania zo súboru program prejde celým súborom a čaká na ukončenie stlačením ľubovolnej klávesy. V prípade čitania paketov z rozhrania, je potrebné aby užívatel ukončil program stlačením CTRL^C.

Prefixy musia byť v tvare N.N.N.N/P, kde N je celé číslo v rozsahu 0-255 a P je celé číslo v rozsahu 0-30, P pre čísla 31 a 32 nemá význam, nakoľko pre P=31 je 0 voľných adries a pre P=32 je -2 voľných adries.

Príklad použitia:

./dhcp-stats -r dhcp.pcap 192.168.1.0/24 192.168.0.0/22 172.16.32.0/24

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

4 Použité zdroje

- https://tldp.org/HOWTO/NCURSES-Programming-HOWTO/helloworld.html
- https://www.ietf.org/rfc/rfc2131.txt
- https://en.wikipedia.org/wiki/Dynamic_Host_Configuration_Protocol
- https://www.gnu.org/software/libc/manual/html_node/Syslog-Example.html
- https://liw.fi/manpages/