



Vysoké Učení Technické v Brně  
Fakulta Informačních Technologii

Projektová dokumentácia k predmetu ISA

# Monitorovanie DHCP komunikácie

# Obsah

<b>1. Úvod.....</b>	<b>3</b>
1.1. DHCP.....	3
1.2. Štruktúra DHCP Paketu.....	3
1.3. Pridelenie adresy.....	4
<b>2. Návrh riešenia.....</b>	<b>5</b>
<b>3. Implementácia.....</b>	<b>6</b>
3.1. Odchyt komunikácie.....	6
3.2. Analýza.....	7
3.3. Použitie.....	7
3.4. Príklady.....	8
<b>4. Zdroje.....</b>	<b>8</b>

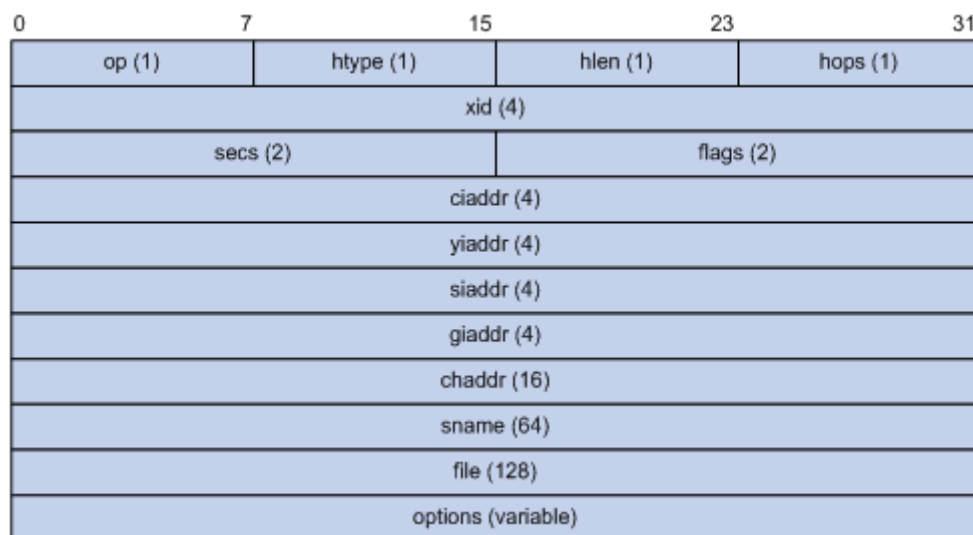
# 1. Úvod

Cieľom projektu je vytvoriť program, ktorý by umožňoval získavanie štatistík o vytiažení sieťového prefixu z pohľadu množstva alokovaných IP adries. V praxi sa daný problém rieši analýzou logových súborov DHCP serveru, alebo túto štatistiku priamo server poskytuje. Naším cieľom je dostupnosť štatistík v prípade, keď DHCP server takúto možnosť nepodporuje a pre ich získanie je treba použiť analýzu sieťovej komunikácie.

## 1.1. DHCP

Dynamic Host Configuration Protocol je protokol bežiaci na aplikačnej vrstve TCP/IP stacku nad UDP (porty 67 a 68). Jedná sa o protokol, ktorý zaisťuje dynamické prideľovanie IP adries v sieti a zasielanie konfiguračných parametrov ako je napríklad maska siete, adresa siete, implicitná brána a adresa DNS serveru. DHCP prideľuje adresy zakaždým, keď sa nejaké zariadenie pripojí do siete, čím eliminuje nutnosť manuálnej konfigurácie IP adresy pre každého klienta.

## 1.2. Štruktúra DHCP Paketu



Obr. 1. štruktúra DHCP paketu<sup>1</sup>

**op** typ správy (1-REQUEST, 2-REPLY)

<sup>1</sup>

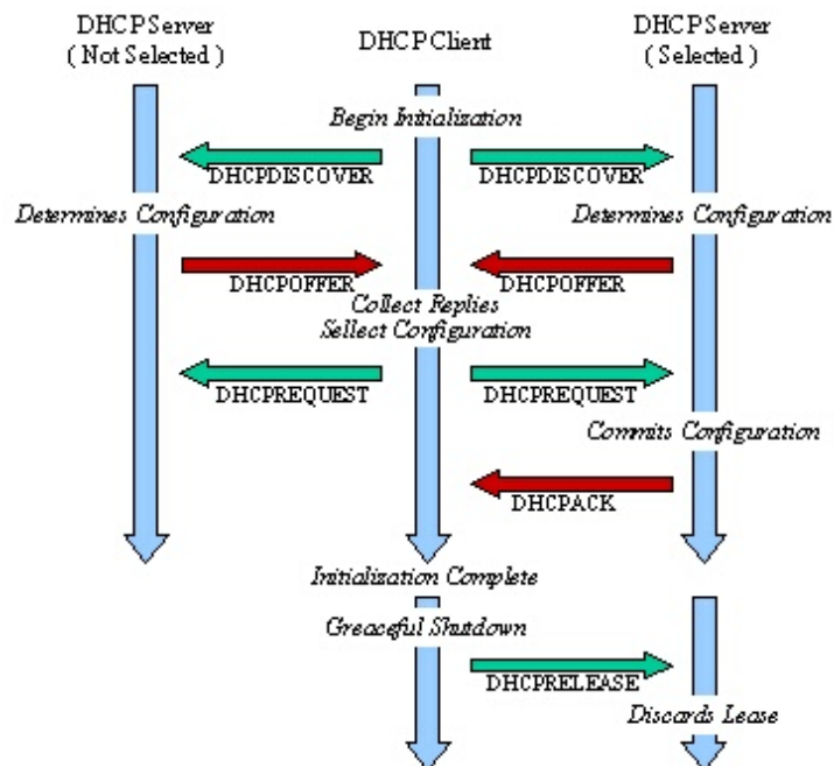
[https://techhub.hpe.com/eginfolib/networking/docs/switches/5120si/cg/5998-8491\\_I3-ip-svcs\\_cg/content/436042653.htm](https://techhub.hpe.com/eginfolib/networking/docs/switches/5120si/cg/5998-8491_I3-ip-svcs_cg/content/436042653.htm)

<b>htype</b>	typ hardwarovej adresy
<b>hlen</b>	dĺžka hardwarovej adresy
<b>hops</b>	počet skokov (pre DHCP relay)
<b>xid</b>	id transakcie, náhodné vygenerované číslo
<b>secs</b>	počet sekúnd ubehnutých od začiatku procesu pridelovania/ obnovenia adresy
<b>flags</b>	príznaky (broadcast alebo unicast)
<b>ciaddr</b>	IP adresa klienta
<b>yiaddr</b>	IP adresa pridelená klientovi serverom
<b>siaddr</b>	IP adresa serveru od ktorého klient obdržal konfiguračné parametre
<b>giaddr</b>	IP adresa prvého “relay agenta”, cez ktorého správa prešla
<b>chaddr</b>	hardwarová adresa klienta
<b>sname</b>	meno serveru od ktorého klient obdržal konfiguračné parametre
<b>file</b>	“bootfile” a informácia o ceste, definuje server pre klienta
<b>options</b>	voliteľné parametre premennej dĺžky, patrí sem napríklad <code>message type</code> , ktorý určuje typ DHCP správy alebo <code>server identifier</code> , ktorý obsahuje adresu serveru, ktorý poskytol pridelenú adresu

### 1.3. Pridelenie adresy

Komunikáciu iniciuje zariadenie [1], ktoré sa chce pripojiť do siete (klient) tým, že na sieť vyšle DHCP DISCOVER [Obr. 2.1] paket so zdrojovou IP adresou 0.0.0.0 a broadcastovou MAC adresou (FF-FF-FF-FF-FF-FF). Všetky DHCP servery, ktoré sa nachádzajú v danej sieti odpovedajú správou DHCP OFFER, pričom ako `yiaddr` nastaví hodnotu adresy, ktorú poskytujú klientovi a v `options` zašlú ďalšie konfiguračné parametre, ako je napríklad hodnota `lease time`, atď. Klient si vyberie jednu z ponúkaných adries, broadcastom zašle správu DHCP REQUEST, pričom `option 50` (requested IP address) [2] nastaví na hodnotu vybranej IP, `option 54` (server identifier) nastaví na hodnotu IP adresy DHCP serveru, od ktorého danú ponuku obdržal. Server potom odpovedá správou DHCP ACK, v ktorej zašle všetky konfiguračné parametre siete (rovnaké ako v DHCP OFFER správe) a zároveň tým potvrdí alokovanie danej adresy. V tomto momente si klient svoje

sieťové rozhranie nastaví na základe obdržaných parametrov a môže sa pripojiť na internet.



Obr.2. Priebeh DHCP komunikácie pri pridelovaní adresy<sup>2</sup>

## 2. Návrh riešenia

Riešenie bude pozostávať z dvoch častí, pričom prvá sa zaoberá zberom paketov a druhá ich analýzou. V tomto riešení budem uvažovať, že DHCP správa bude vždy zabalená v UDP hlavičke so štandardnými DHCP portami 67 a 68, tento datagram v IPv4 hlavičke a tá v Ethernet rámci. Na základe tohto budeme môcť vyselektovať pakety relevantné pre naše riešenie a ďalej s nimi pracovať.

Pri samotnej analýze využijem hlavne položky `yiaddr` a `options`, ktoré DHCP paket obsahuje. Pri prijatí DHCP správy sa najskôr zistí o aký typ sa jedná. V prípade ACKu, ktorým sa potvrdzuje pridelenie adresy [1] sa obsah `yiaddr` započíta do štatistík pre sledované prefixy. Vyťaženosť prefixu je daná vzorcom

$$utilization = \frac{allocated}{max\_addrs} * 100\%$$

<sup>2</sup> IPK Slidy 2022 - IPv4 (Veselý)

kde `allocated` je počet alokovaných adries daného prefixu a `max_addrs` je maximálny počet adries daného prefixu, tj.  $max\_addrs = 2^{32-prefix} - 2$ .

### 3. Implementácia

Samotný program je napísaný v jazyku C++ a testovaný na referenčnom stroji `merlin`. Pre prehľadnosť zdrojového kódu som logiku aplikácie rozdelila do viacerých súborov.

<code>main.c</code>	spracovanie vstupných argumentov využitím <code>getopts</code> , vytvorenie inštancie analyzátoru, výpis do terminálu pomocou <code>ncurses</code>
<code>dhcp.*</code>	definícia štruktúry DHCP paketu a pomocné funkcie na vyhľadávanie v <code>options</code>
<code>dhcp-stats.*</code>	trieda <code>DHCPAnalyzer</code> , definície jednotlivých metód pre prácu s prichádzajúcimi paketmi
<code>subnet.*</code>	trieda <code>Subnet</code> , definície funkcií pre prácu s IP prefixami, výpočet štatistík pre jednotlivé prefixy

#### 3.1. Odchyt komunikácie

Na odchyt komunikácie som použila knižnicu `libpcap` [3]. Ak je program spustený v offline móde, komunikácia sa načíta zo zadaného `.pcap` súboru pomocou funkcie `pcap_open_offline`. Pri online režime sa záchyt paketov vykonáva prostredníctvom funkcie `pcap_open_live` na zadanom rozhraní. Na filtrovanie paketov relevantných pre danú aplikáciu som nastavila filter s hodnotou `"udp port 67 or udp port 68"`, ktorý spôsobí, že pri volaní funkcie `pcap_next` (čítanie ďalšieho paketu) nám budú vždy navrátené iba pakety, ktoré obsahujú DHCP komunikáciu bežiacu na štandardných UDP portoch 67 a 68.

## 3.2. Analýza

Prvým krokom je oddelenie DHCP správy od hlavičiek protokolov vyšších vrstiev, tj. Ethernet, IP UDP. Túto činnosť vykonáva funkcia `DHCPAnalyzer::strip_payload`. Stredom analýzy je funkcia `DHCPAnalyzer::interpret_dhcp_message`, ktorá v prvom rade zistí, o aký typ DHCP správy sa jedná na základe `option message type (53)` v časti `options`. Hľadanie položiek v DHCP options má na starosť funkcia `get_dhcp_option` z `dhcp.c` volaná s príslušnými parametrami.

Ak sa jedná o typ správy ACK, volá sa funkcia `DHCPAnalyzer::update_subnet_stats`, ktorá najskôr sa skontroluje, či hodnota `yiaddr` danej správy už existuje v poli `addrs`, t.j. či už daná adresa bola pridelená a jedná sa len o ACK ako reakcia na predĺženie `lease time` a podobne. Ak sa hodnota `yiaddr` v poli nenachádza, vloží sa na koniec tohto pola. Zároveň sa u každého sledovaného prefixu skontroluje, či hodnota `yiaddr` spadá do rozsahu daného prefixu (funkcia `Subnet::contains`). Ak áno, navýši u neho počítadlo alokovaných adries o jedna.

Ak pridelenie novej adresy spôsobí, že vyťaženosť nejakého z prefixov presiahne 50%, vypíše sa do terminálu správa "`prefix xy exceeded 50% of allocations`". Rovnaká správa sa zapíše aj do systémového logu.

## 3.3. Použitie

Pre preklad zdrojových súborov je potrebné zavolať príkaz `make` v adresári obsahujúcom súbor `Makefile` pre danú aplikáciu. Ten vytvorí spustiteľný súbor `dhcp-stats` v tom istom adresári. Spustiť samotnú aplikáciu je možné príkazom nasledujúceho formátu,

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

kde

<code>-r &lt;filename&gt;</code>	názov pcap súboru, ktorý sa má spracovať
<code>-i &lt;interface-name&gt;</code>	názov rozhrania, na ktorom sa má spustiť odposluch

<ip-prefix>                      adresa siete s prefixom, ktorej štatistika sa má počítať  
pričom aplikácia očakáva, že bude vždy zadáný práve jeden z parametrom `-r` a `-i`,  
t.j. vždy bude pracovať buď v offline alebo online režime. IP prefixov môže  
nasledovať ľubovoľné množstvo a môžu sa rozsahovo prekryvať.

V prípade správne zadaných parametrov sa v terminálovom okne spustí  
aplikácia. V online režime sa vypísané štatistiky prepočítajú pri každom novom  
zачytenom pakete a v offline režime zostávajú nemenné až po ukončenie aplikácie.  
Ukončiť aplikáciu v oboch režimoch je možné signálom `SIGINT`, resp. stlačením  
`CRTL+C`.

### 3.4. Príklady

```
$ ./dhcp-stats -r examples/dhcp.pcap 192.168.1.0/26  
172.16.32.0/24 192.168.0.0/22
```

výstup:

IP-Prefix	Max-hosts	Allocated addresses	Utilization
192.168.1.0/26	62	50	80.65%
172.16.32.0/24	254	0	0.00%
192.168.0.0/22	1022	50	4.89%
prefix 192.168.1.0/26 exceeded 50% of allocations			

```
$ ./dhcp -r examples/mynetwork.pcap 192.168.0.0/24  
192.168.1.0/23
```

výstup:

IP-Prefix	Max-hosts	Allocated addresses	Utilization
192.168.0.0/24	254	1	0.39%
192.168.1.0/23	510	1	0.20%

## 4. Zdroje

[1] Droms R., *Dynamic Host Configuration Protocol*. RFC 2131. Mar. 1997.  
URL: <https://datatracker.ietf.org/doc/html/rfc2131>

[2] Alexander S., Droms R. *DHCP Options and BOOTP Vendor Extensions*.  
RFC 2132. Mar. 1997. URL: <https://datatracker.ietf.org/doc/html/rfc2132>



[3] Cartens T. *Programming with pcap*. online. 2002. URL:  
<https://www.tcpdump.org/pcap.html>