Vysoké učení technické v Brně
Fakulta informačních technologií

Síťové aplikace a správa sítí – monitorování DHCP komunikace

Manuál k programu dhcp-stats

16. listopadu 2023

Ondřej Koumar (xkouma02)

Obsah

Úvod

Ne vždy má uživatel možnost sledovat statistiku vytížení síťových prefixů. Některé DHCP servery tuto statistiku poskytují samy, případně se mohou parsovat adresy z jejich logů. Pokud ale takováto možnost není, nezbývá moc jiných možností, než sledovat DHCP provoz odchytáváním paketů a manuálním parsováním IP adres, které jsou klientským stanicím přidělovány. To je use-case, pro který byl program `dhcp-stats` vytvořen.

Program `dhcp-stats` je schopen monitorovat DHCP provoz na vybraném rozhraní, ať už se jedná o ethernetové či bezdrátové, a generovat statistiku pro uživatelem zadaný síťový prefix. Samotné monitorování spočívá v odchytávání a filtraci paketů, které na daném rozhraní projdou, a hledání podstatných informací v nich. V paketu, který je odeslán DHCP serverem, případně klientem, který DHCP službu využívá, jsou umístěny veškeré informace, které jsou potřebné pro generování statistiky pro síťový prefix.

Pokud uživatel nemá potřebu přímo monitorovat DHCP provoz naživo, má možnost využít zpracování *.pcap* nebo *.pcapng* souborů (které si může vygenerovat například pomocí programu Wireshark[1]). To se hodí například v případě, že má již síť zmonitorovanou a nepotřebuje real-time statistiku. V tomto případě je ale počítat s tím, že možnosti programu jsou omezené; vypíše se pouze finální podoba sítě, tedy vytížení prefixů v době, kdy skončilo zachytávání paketů. Je ale možné do programu uměle vložit zpoždění tak, aby šlo vidět zpracování paketů po jednom. Více o této možnosti v kapitole 3.

[1] O programu se dozvíte na https://www.wireshark.org/about.html.

1 Uvedení do problematiky

DHCP (*Dynamic Host Configuration Protocol*) je popsán v rámci RFC 2131. DHCP se skládá za dvou částí – z protokolu zajišťujícího doručování parametrů od serveru ke klientovi a systém alokací IP adres. Je postaven na modelu klient-server, kde server je zařízení, které poskytuje parametry přes přenosovou část protokolu a klient je zařízení, které o tyto parametry DHCP server žádá.

1.1 DHCP pakety

Položky DHCP paketu a jejich vysvětlení:

Pole	**Velikost (B)**	**Popis**
`op`	1	Kód operace zprávy.
`htype`	1	Typ hardwarové adresy.
`hlen`	1	Délka hardwarové adresy.
`hops`	1	Počet relay agentů[2], přes které šla DHCP zpráva.
`xid`	4	ID transakce, které používají jak server, tak klient k identifikaci zpráv.
`secs`	2	Počet sekund od začátku transakce (žádost o adresu nebo obnovení *lease time*).
`flags`	2	Příznak broadcastu.
`ciaddr`	4	IP adresa klienta.
`yiaddr`	4	Nová klientova IP adresa (použito při nabízení a potvrzování adres od serveru).
`siaddr`	4	IP adresa serveru, který má klient kontaktovat při další zprávě.
`giaddr`	4	IP adresa relay agenta, přes kterého se posílají DHCP zprávy.
`chaddr`	16	MAC adresa klientovy síťové karty.
`sname`	64	Jméno serveru (volitelné).
`file`	128	Název souboru, který klient použije pro bootstrapping[3].
`options`	n	Pole volitelných parametrů.

Tabulka 1: Formát zprávy DHCP

Poznámky:

- `op` Může nabývat hodnot BOOTREQUEST a BOOTREPLY.
- Výčet typů hardwarových adres zde.
- `xid` je náhodné číslo generované klientem, používá se po celou dobu komunikace.
- `flags` je ve formátu:

Bits	**Value**
0	B
1-15	MBZ

Tabulka 2: `flags` pole

kde *B* je příznak, že zpráva byla poslána na broadcastovou adresu sítě, *MBZ* je 15 bitů, které jsou vždy nastaveny na 0.

[2] V kontextu DHCP se jedná o proces získání potřebných informací od DHCP serveru.
[3] Relay agenti mají na starost přeposílání paketů mezi klientem a serverem při DHCP komunikaci.

- `options` je proměnné velikosti, klient ale musí být připraven přijmout DHCP zprávu, která má velikost `options` alespoň 312 B. Ne všechny parametry se do pole `options` musí vlézt; pokud je třeba, DHCP server může využít pole `sname` případně pole `file` pro uložení zbývajících parametrů. Pro výčet parametrů, které se v tomto poli mohou vyskytnout, vizte zde.

1.2 DHCP komunikace

1.2.1 DHCP zprávy

Před vysvětlením samotné komunikace je potřeba základní výčet zpráv, které si klient a server v rámci DHCP posílají.

Zpráva	**Využití**
DHCPDISCOVER	Klientovo vysílání pro nalezení dostupných serverů.
DHCPOFFER	Odpověď serveru na DHCPDISCOVER s nabídkou konfiguračních parametrů.
DHCPREQUEST	Může mít několik různých významů: • Klient nemá problém s nabídnutými parametry v DHCPOFFER, zažádá o ně tedy v rámci této zprávy. • Klient se ptá na správnost dříve přidělené adresy po např. restartu systému. • Klient chce prodloužit pronájem (*lease time*) již používané síťové adresy. Kompletní přehled a více informací zde.
DHCPACK	Posílá server, obsahuje konfigurační parametry (1.1) pro klienta do sítě.
DHCPNAK	Posílá server, oznamuje, že server nesouhlasí s parametry, o které si klient zažádal v DHCPREQUEST.
DHCPDECLINE	Posílá klient a oznamuje, že IP adresa je již používána.
DHCPRELEASE	Posílá klient, ruší pronájem IP adresy (z různých důvodů).
DHCPINFORM	Posílá klient a ptá se, jaké má lokální konfigurační parametry, přičemž adresa mu již byla přidělena externě.

Tabulka 3: Typy DHCP zpráv a jejich využití

1.2.2 Posloupnost zpráv

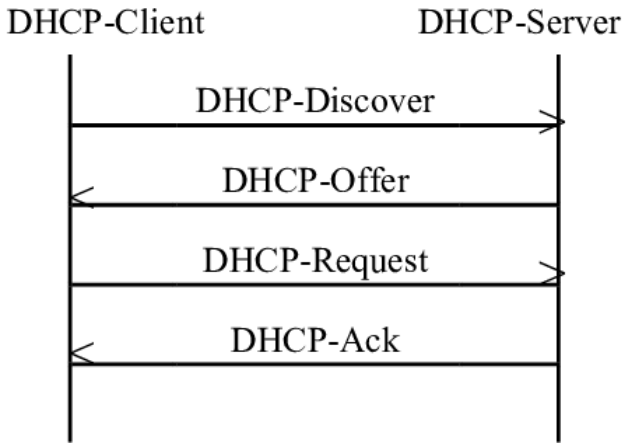
Komunikaci začíná klient tím, že na obecný broadcast[4] vyšle DHCPDISCOVER zprávu. DHCP server tuto zprávu přečte, podívá se na adresy, co má k dispozici a zprávou DHCPOFFER nabídne novému klientovi síťovou konfiguraci. Také do této zprávy na políčko `siaddr` vloží svoji IP adresu, aby mohl být server identifikován po zaslání DHCPREQUEST na broadcast.

Klient se na konfiguraci podívá a pokud mu vyhovuje, oficiálně o tuto konfiguraci zažádá zprávou DHCPREQUEST. Server může přijmout žádost, a tedy poslat potvrzovací DHCPACK zprávu, nebo odmítnout a poslat DHCPNAK zprávu.

V prvním případě má klient ještě možnost odmítnout zprávou DHCPDECLINE, pokud adresu již některé zařízení v síti používá. V tomto případě se klient vrací do stavu, kdy komunikace se serverem probíhá od začátku zprávou DHCPDISCOVER. Pokud ne, adresu přijme a může ji používat v lokální síti. Další komunikace proběhne až klient bude rušit pronájem adresy (případně při zprávě DHCPINFORM).

[4]Protože klient nezná prefix lokální sítě, je zvolena adresa, které rozumí všechna zařízení, a to 255.255.255.255.

V druhém případě se klient vrací do fáze, kdy znovu vysílá DHCPDISCOVER zprávu a komunikace se serverem probíhá od začátku.



Obrázek 1: Typická posloupnost DHCP zpráv s jedním serverem.[1]

Nezapomeňme, že v dosahu se DHCP serverů může vyskytovat více; klient si v tom případě zvolí jeden z nich a jeho adresu vloží do pole `siaddr`, aby se server mohl identifikovat. DHCPREQUEST je také posílán na obecný broadcast a servery musí vědět, komu zpráva patří. Pokud DHCPREQUEST není určen serveru, pak jeho komunikace v tomto bodě končí.

Po vypršení *lease time*, jenž je v DHCP packetu v poli `options` s číslem 51, případně pokud se klient sám rozhodne z jiných důvodů zrušit pronájem IP adresy, klient posílá zprávu DHCPRELEASE. Typicky klient kontaktuje stejný server[5] zprávou DHCPREQUEST se stejnou adresou, jako používal do této chvíle. Server může přijmout, a tedy zaslat DHCPACK, případně odmítnout a klient započíná proces získávání IP adresy od začátku zprávou DHCPDISCOVER.

2 Návrh aplikace

Aplikace je objektově orientovaná, a proto je implementována v C++. V aplikaci jsou 4 třídy:

- **ArgumentProcessor** má za úkol zpracovávat argumenty příkazové řádky, které byly programu předány. Kontroluje pouze správnost přepínačů a návratovou hodnotu od IpAddressParseru.
- **IpAddressParser** je pomocníkem ArgumentProcessoru. Z Argumentů příkazové řádky kontroluje správnost IP adres, které byly programu předány.
- **PacketSniffer** uchovává informace o použitém rozhraní, případně souboru, ze kterého se načítá, dále data a hlavičky paketů a další pomocné struktury potřebné pro čtení paketů. Extrahuje IP adresy z paketu a předává je IpAddressManageru.
- **IpAddressManager** je hlavní datovou strukturou programu. Uchovává si informace o každé síti, která byla předána jako argument příkazové řádky. Podporuje přidávání i odebírání adres ze sítí.

[5] Opět na broadcast, tentokrát ale lokální sítě.

Dále se v aplikaci nachází datová struktura **NetworkData**. V této struktuře jsou uchovávány veškeré parametry sítě, například:

- adresa,
- maska,
- broadcastová adresa,
- počet obsazených adres,
- obsazené adresy,
- obsazenost v % a další.

S vektorem těchto datových struktur pracuje IpAddressManager.

Program je uzpůsoben tomu, aby při přijmutí signálů *SIGINT* a *SIGTERM* byl bezpečně ukončen. Vypisování informací o sítích je řešeno knihovnou ncurses. Při překročení 50 % vytížení prefixu se standardní logovací rutinou `syslog` zaloguje tato informace do systémového logu. Detailnější popis v sekci 3.

3 Popis implementace

Program je spuštěn funkcí `main`, která se nachází v souboru *dhcp-stats.cpp*. Volá ArgumentProcessor pro zpracování argumentů, poté PacketSniffer, aby začal zpracovávat pakety na rozhraní, případně v souboru.

3.1 ArgumentProcessor

3.2 IpAddressParser

3.3 PacketSniffer

3.4 IpAddressManager

4 Základní informace o programu

5 Návod na použití

Reference

[1] Lukas Pürgstein and Hans-Joachim Hof. A system to save the internet from the malicious internet of things at home. In *The Eleventh International Conference on Emerging Security Information, Systems and Technologies (SECURWARE 2017)*, page 184, 09 2017. `https://www.researchgate.net/figure/Typical-DHCP-sequence_fig2_319932617` [accessed 15 Nov, 2023].