Dokumentace k projektu

Monitorování DHCP komunikace

2023/2024

Síťové aplikace a správa sítí (ISA)

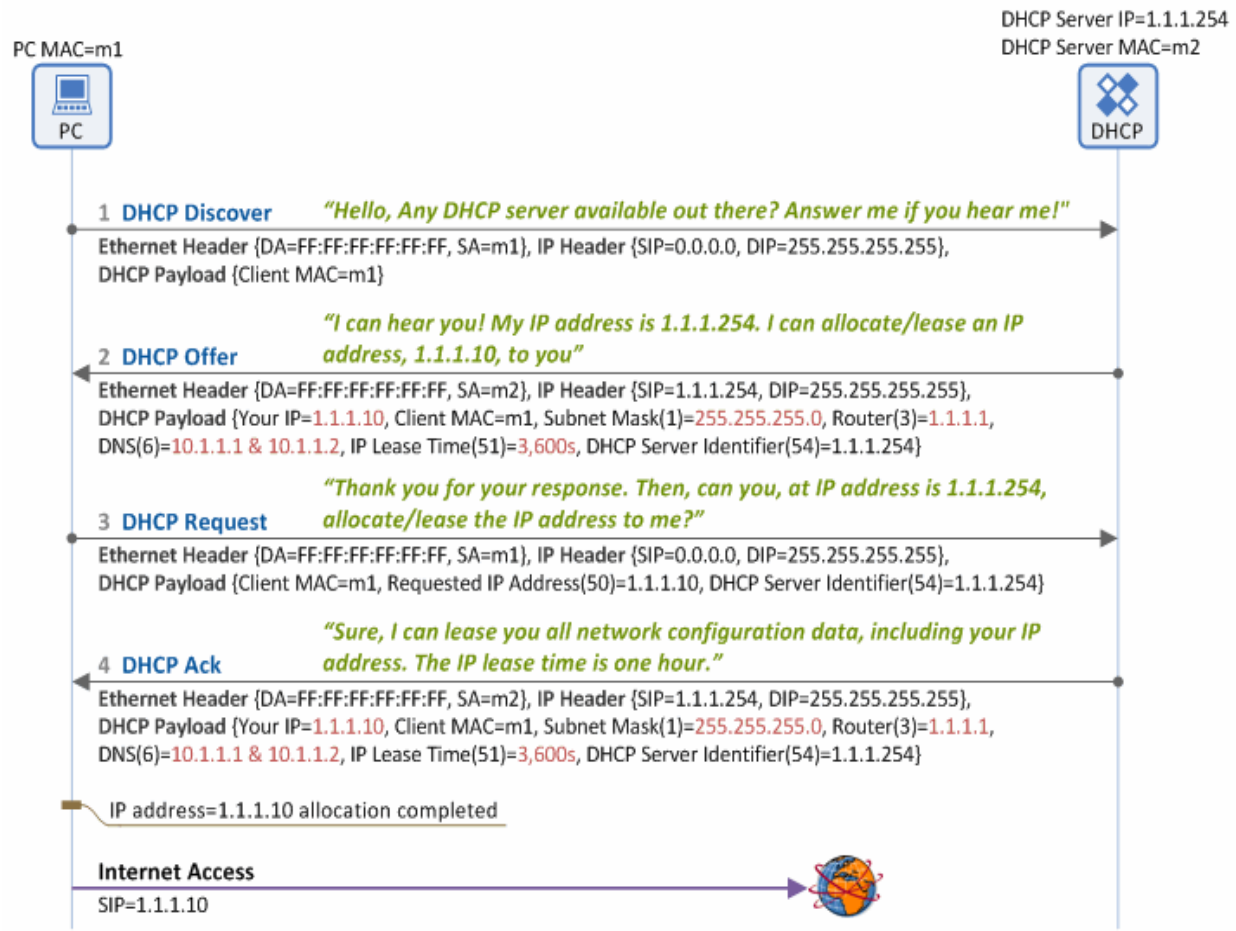
Autor: Kateřina Čepelková, xcepel03
Datum: 17. listopadu 2023

1 Obsah

2 Úvod do problematiky

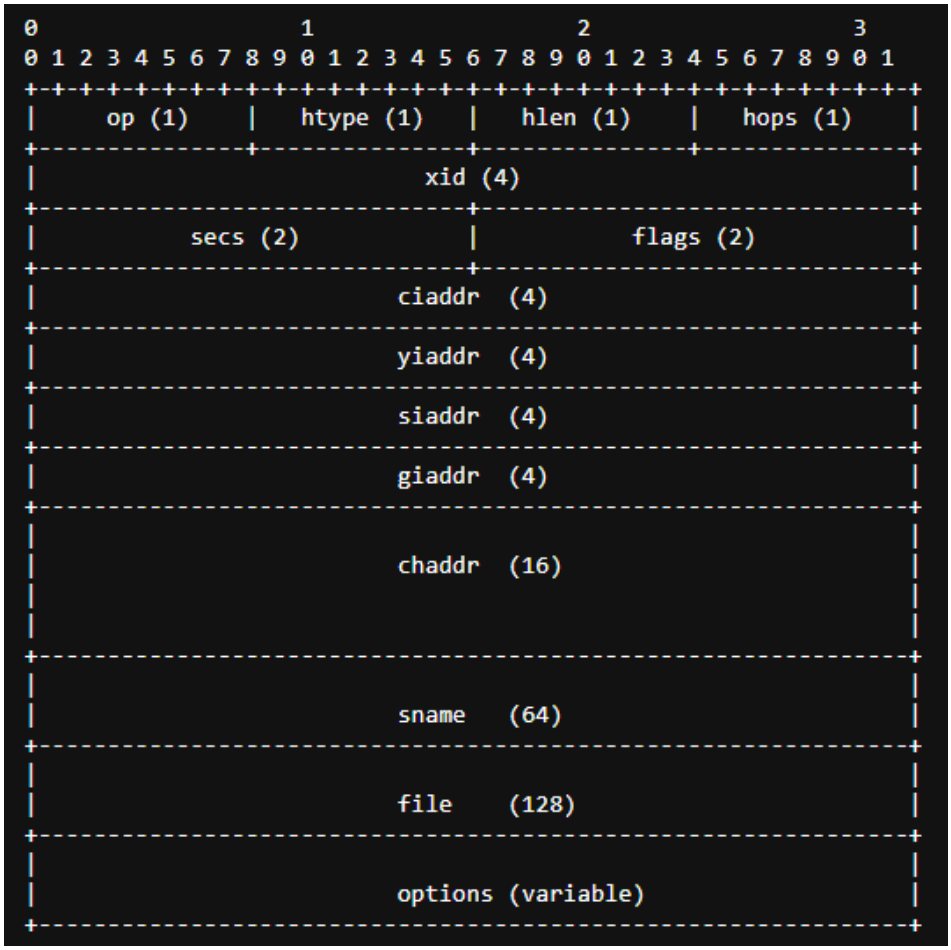
DHCP neboli „Dynamic Host Configuration Protocol“ je v oblasti informatiky protokol z rodiny TCP/IP používaný pro automatickou konfiguraci počítačů připojených do počítačové sítě[1]. Konfigurace probíhá pomocí klient-server architektury. DHCP protokol umožňuje díky DHCP serveru nastavit stanici v počítačové síti sadu parametrů nezbytných pro komunikaci pomocí IP protokolu[2].

Komunikace mezi serverem a klientem probíhá na UDP portech 68 (klient) a 67 (server)[3]. Komunikace probíhá ve 4 vlnách – DHCP Discover (klient hledá DHCP server, ke kterému by se mohl připojit), DHCP Offer (DHCP server nabízí klientovi volnou adresu, kterou by pro něj mohl alokovat), DHCP Request (klient odpovídá, že s adresou souhlasí), DHCP ACK (server potvrzuje klientovi, že mu propůjčuje danou adresu)[4].



Obrázek 1 – Komunikace DHCP serveru a klienta

[1] JasonGerend Dynamic Host Configuration Protocol (DHCP). In: Microsoft Learn. [cit. 2023-10-23]. Dostupné z: https://learn.microsoft.com/en-us/windows-server/networking/technologies/dhcp/dhcp-top.
2 Lemon, Ted; Droms, Ralph. The DHCP handbook. Indianapolis: SAMS, 2003. ISBN 0-672-32327-3.
3 Writer CBT, BasuMallick C, Writer T, et al (2022) The role of DHCP (Dynamic Host Control Protocol) in Networking. In: Spiceworks. [cit. 2023-10-23]. Dostupné z: https://www.spiceworks.com/tech/networking/articles/what-is-dhcp/.
4 In: Understanding the basic operations of DHCP | NETMANIAS - Network manias. [cit. 2023-10-23]. Dostupné z: https://www.netmanias.com/en/?m=view&id=techdocs&no=5998&vm=pdf.



Obrázek 2 – Formát DHCP paketu

Popis důležitých parametrů:[5]

- op = operační kód zprávy (1 = BOOTREQUEST – zpráva klienta serveru, 2 = BOOTREPLY – zpráva od serveru klientovi)
- yiaddr = přiřazená IP adresa, vyplněná použitelnou hodnotou pouze u ACK zprávy, jinak 0.0.0.0
- options = seznam možností zapsaných za sebou ve formátu kód volby (1 byte) – délka informací (1 byte) – informace (x bytů)
    - kód 53 = Typ zprávy DHCP (1 DHCPDISCOVER, 2 DHCPOFFER, 3 DHCPREQUEST, 4 DHCPDECLINE, 5 DHCPACK, 6 DHCPNAK, 7 DHCPRELEASE, 8 DHCPINFORM)[6]

[5] Droms R (1997) RFC 2131: Dynamic Host Configuration Protocol. In: IETF Datatracker. [cit. 2023-10-23]. Dostupné z: https://datatracker.ietf.org/doc/html/rfc2131?fbclid=IwAR3XTdlVbwVcEw2Vhn5BXx33UVqhpFuk__nGIYGJuoLZbpw5i9s9YOGiytc#ref-19.
[6] Droms R, Alexander S (1997) RFC 2132: DHCP options and BOOTP Vendor extensions. In: IETF Datatracker. [cit. 2023-10-23]. Dostupné z: https://datatracker.ietf.org/doc/html/rfc2132.

3 Základní informace o programu

Program je vytvořen v jazyce C++ a má za úkol monitorovat obsazenost síťových adres pomocí sledování DHCP paketů. Lze ho spustit na uživatelem zvoleném síťovém rozhraní, na kterém bude naslouchat a aktualizovat statistiky dle přicházejících paketů. Alternativně může také zpracovat pcap soubor a generovat statistiku z uloženého záznamu síťové komunikace.

Statistika je generována v příkazovém řádku ve formátu IP prefix – Maximální množství alokovaných IP adres – Počet alokovaných IP adres – Úroveň vytížení (%). V případě, že počet alokovaných adres s konkrétním prefixem překročí 50 % z maximálního počtu, program automaticky pošle pomocí syslogu informační log se záznamem a identifikací prefixu, u kterého bylo toto překročení zjištěno a zároveň ho vypíše na standartní výstup.

4 Návrh aplikace a implementace

Prvním krokem programu je zpracování argumentů zadané uživatelem. To se děje ve funkci `int args_handle()`. *Tam jsou tyto argumenty pečlivě překontrolovány* a pokud odpovídají očekávaným podmínkám, je navrácena hodnota 0, v opačném případě navrátí 1. Těmito podmínkami je, že uživatel musí zadat alespoň jeden z dvojice pcap soubor a síťové rozhraní a minimálně jeden IP prefix ve formátu IPv4. Tyto prefixy jsou ihned po validaci korektní formy pomocí regexu, zpracovány funkcí `void prefix_analyze()` do struktury `prefix`, která obsahuje důležité informace.

```
struct prefix {
    string full; // prefix ve formě řetězce pro snadný výstup
    int netmask; // síťová maska prefixu
    uint32_t subnet; // podsíť prefixu uložena jako 32bitového binárního čísla
    uint32_t mask; // maska pro logický výpočet na vyhledávání IP adres s daným prefixem
    int maxHosts; // maximální počet alokovaných adres = 2^(32 – netmask) – 2 (kvůli
                  broadcastu a adrese serveru)
    int occupied = 0; // počet již obsazených adres
    double utilization = 0; // vytíženost v procentech = (occupied/maxHosts) * 100
    bool warned = false; // kontrola, zda již bylo vytisknuto varování o překročení 50 %
                         zaplnění
};
```

Po zpracování argumentů je inicializováno okno pomocí knihovny `ncurses.h`, které je následně nakonfigurováno funkcí `void win_setup()`. Tato funkce nastaví hlavní lištu okna podle nejdelšího možného záznamu nebo hlavičky každého sloupce. Zároveň jsou zde inicializovány všechny počáteční hodnoty zadaných IP prefixů z jejich struktury a to pomocí funkce `void win_update()`, která je používána i později v kódu k průběžné aktualizaci tohoto okna.

Kód se nadále větví do 2 řešení podle toho, zda byla vybrána online verze (bylo zadáno rozhraní) či offline (byl zadán soubor). V obou případech je pomocí `pcap.h` knihovny správně nakonfigurované připojení/otevření souboru. Následně se iteruje skrze pakety, které jsou zpracovány ve funkci `void packet_handle()`. Pro správnou identifikaci DHCP packetů s ACK zprávou je kontrolováno, zda paket obsahuje UDP hlavičku a jestli je jeho zdrojový port 67 a jeho cílový port 68. Takto zůstanou pouze pakety se zprávou ACK a Offer.

Pro nalezení pouze ACK zpráv je provedena analýza voleb `options` DHCP paketu, kde je hledán kód 53, neboli typ zprávy. Není ale garantované, že se tento kód bude vždy nacházet na stejné pozici,[7] proto je nutné postupně projít všechny volby paketu a zkontrolovat všechny kódy. Pokud kód nemá hodnotu 53, zjistíme z dalšího bytu délku informace v bytech a posuneme se na další kód. Toto je opakováno, dokud není nalezen kód 53, či konec paketu. V případě nalezení kódu 53 je následně zjištěno, zda se jedná o ACK zprávu (hodnota 5). Pokud se jedná o ACK zprávu, pak byl identifikován správný paket, který přenáší informaci s alokovanou IP adresou v `yiaddr`, která se nachází v DHCP paketu od 16. bytu. V případě, že se jedná o dosud nezaznamenanou IP adresu (ještě není zapsána v množině IP adres `set<uint32_t> ipAdresses)`, je následně adresa uložena ve formě 32bitového čísla.

[7] *Are DHCP options* ordered? | Stack Overflow. [online]. Copyright © 2023 [cit. 2023-10-23]. Dostupné z: https://stackoverflow.com/questions/77033547/are-dhcp-options-ordered

Pro toto číslo je následně zkontrolována kompatibilita s každým IP prefixem ve funkci `void check_compatibility()`. Kontrola je provedena pomocí maskování IP adresy s maskou sítě odpovídající danému IP prefixu. Pokud se vymaskovaná hodnota shoduje s adresou prefixu, je adresa započítána do celkového obsazení prefixu a dle toho je i aktualizováno vytížení. Po vyhodnocení je zavolána funkce `void win_update()` pro obnovení okna.

5 Návod a použití

Program je nutné přeložit pomocí příkazu `make` a následně se spouští pomocí příkazu `./dhcp-stats [-r <filename>] [-i <interface-name>] <ip-prefix> [ <ip-prefix> [ ... ] ]`
Program je třeba spouštět s potřebnými právy pro naslouchání na daných portech (např. pomocí `sudo` u platformy Linux).

Je nutné zadat pouze jeden z dvojice přepínačů `[-r <filename>]` a `[-i <interface-name>]`, při zadání obou bude program ukončen s chybovým hlášením.

IP prefixů je možné zadat neomezený počet, ale musí být zadán alespoň 1, jinak bude program ukončen s chybovým hlášením.

Popis parametrů

- `-r <filename>` – pcap soubor, ze kterého se bude tvořit statistika (offline verze)
- `-i <interface>` – rozhraní, na kterém bude program naslouchat a tvořit statistiku (online verze)
- `<ip-prefix>` – podsíť zadávaná ve formátu IPv4, pro kterou bude generována statistika
- `-h` – nápověda

Po spuštění programu se uživateli zobrazí výstupní okno, kde budou vypsané statistiky. Pro ukončení programu může uživatel využít klávesovou zkratku `Ctrl + C`.

6 Bibliografie

Citace

1. JasonGerend Dynamic Host Configuration Protocol (DHCP). In: Microsoft Learn. [cit. 2023-10-23]. Dostupné z: https://learn.microsoft.com/en-us/windows-server/networking/technologies/dhcp/dhcp-top.
2. Lemon, Ted; Droms, Ralph. The DHCP handbook. Indianapolis: SAMS, 2003. ISBN 0-672-32327-3.
3. Writer CBT, BasuMallick C, Writer T, et al (2022) The role of DHCP (Dynamic Host Control Protocol) in Networking. In: Spiceworks. [cit. 2023-10-23]. Dostupné z: https://www.spiceworks.com/tech/networking/articles/what-is-dhcp/.
4. In: Understanding the basic operations of DHCP | NETMANIAS - Network manias. [cit. 2023-10-23]. Dostupné z: https://www.netmanias.com/en/?m=view&id=techdocs&no=5998&vm=pdf.
5. Droms R (1997) RFC 2131: Dynamic Host Configuration Protocol. In: IETF Datatracker. [cit. 2023-10-23]. Dostupné z: https://datatracker.ietf.org/doc/html/rfc2131?fbclid=IwAR3XTdlVbwVcEw2Vhn5BXx33UVqhpFuk__nGIYGJuoLZbpw5i9s9YOGiytc#ref-19.
6. Droms R, Alexander S (1997) RFC 2132: DHCP options and BOOTP Vendor extensions. In: IETF Datatracker. [cit. 2023-10-23]. Dostupné z: https://datatracker.ietf.org/doc/html/rfc2132.
7. Are DHCP options ordered? | Stack Overflow. [online]. Copyright © 2023 [cit. 2023-10-23]. Dostupné z: https://stackoverflow.com/questions/77033547/are-dhcp-options-ordered

Obrázky

1. In: Cisco Learning Network. [cit. 2023-10-23]. Dostupné z: https://learningnetwork.cisco.com/s/question/0D53i00000Kt6zTCAR/dhcp-offer-message.
2. Droms R (1997) RFC 2131: Dynamic Host Configuration Protocol. In: IETF Datatracker. [cit. 2023-10-23]. Dostupné z: https://datatracker.ietf.org/doc/html/rfc2131?fbclid=IwAR3XTdlVbwVcEw2Vhn5BXx33UVqhpFuk__nGIYGJuoLZbpw5i9s9YOGiytc#ref-19.