VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
FAKULTA INFORMAČNÍCH TECHNOLOGIÍ

Počítačové komunikace a sítě – 2. projekt

ARP Scanner

23. dubna 2017 Karel Ondřej

Obsah

1 Address Resolution Protocol

Address Resolution Protocol (dále ARP) slouží k přiřazení neznámé linkové adresy k síťové adrese v lokální síti. Používá se téměř výhradně pro překlad IP adres na MAC adresy, ale byl navržen pro mnoho různých protokolů síťové vrstvy nebo i jiných typů adres fyzické vrstvi.

1.1 Princip funkce

Zařízení, které chce získat fyzickou adresu cílového zařízení, vyplní ARP žádost a odešle ji na *broadcast* (v Ethernetu je ARP žádost uložena do ethernetového rámce a odeslána na adresu *ff:ff:ff:ff:ff:ff*). Všechny zařízení v lokální síti přijmou ARP žádost (v rámci optimalizace si můžou uložit informace o odesílateli). Pokud byla zařízení určena žádost, tak sestaví ARP odpověď a odešle ji jako *unicast* zdrojovému zařízení.

1.2 Struktura Ethernet rámce

offset	Layer
6	MAC Target
6	MAC Sender
(4)	802.1Q tag (Optional)
2	Type/Length
46 (42) - 1500	Payload
4	CRC

Tabulka 1: Ethernet rámec (linková vrstva)

MAC Target
Adresa identifikující příjemce.

MAC Sender
Adresa identifikující odesílatele.

802.1Q tag
Definice virtuální sítě (VLAN). Volitelná položka.

Tape/Length
Specifikuje obsah datového pole (pro ARP 0x0806).

Payload
Datové pole (může obsahovat např. ARP žádost nebo odpověď).

CRC
Kontrolní součet sloužící k detekci poškození rámce.

1.3 Struktura ARP packetu

bits	0 - 7	8 - F
00	Hardware type	
10	Protocol type	
20	Hardware address length	Protocol address length
30	Operation	
40	Sender hardware address	
50		
60		
70	Sender protocol address	
80		
90	Target hardware address	
A0		
B0		
C0	Target protocol address	
D0		

Tabulka 2: ARP diagram pro IPv4, která používá Ethernet

Hardware type
Specifikace systémového protokolového typu (0x0001 pro Ethernet).

Protocol type
Specifikace vnitřního systémového protokolu (0x0800 pro IPv4).

Hardware address length
Délka hardwarové adresy v bytech (6 pro Ethernet).

Protocol address length
Délka protokolové adresy v bytech (4 pro IPv4).

Operation
Pro žádost nabývá hodnoty 1 a pro odpověď 2.

Sender hardware address
Hardwarová adresa odesílatele. V odpovědi slouží k přiřazení MAC adresy k IP adrese.

Sender protocol address
Protokolová adresa odesílatele.

Target hardware address
Hardwarová adresa příjemce. V ARP žádosti se na ni nebere zřetel (nastavena např. na 00:00:00:00:00:00) a v odpovědi označuje zařízení, které vyvolalo dotaz.

Target protocol address
Protokolová adresa příjemce pro kterou chceme zjistit hardwarovou adresu.

1.4 Bezpečnost

ARP protokol není vhodný pro prostředí se zvýšeným nárokem na bezpečnost, jelikož místo skutečného vlastníka hledané IP adresy může odpovědět útočník. Následně by komunikace neprobíhala s hledaným zařízením, ale s útočníkem.

2 Implementace

ARP skener je vyvinut na systému *Debian*. Jako vstup dostane rozhraní, nad kterým má proběhnout skenování a soubor, kam se má uložit výsledek. K vytvoření RAW socketu jsou potřeba administrátorská práva.

2.1 Inicializace

Aplikace skenuje zařízení s IPv4 adresou v síti Ethernet. Proto se hardwarový typ nastaví na 0x0001 a protokolový typ na 0x0800. Délka adresy pro Ethernet je 6 a délka adresy pro IPv4 je 4. Kód operace pro ARP žádost je 0x0001. MAC adresa a IP adresa zdrojového zařízení na zadaném rozhraní se získá pomocí socketů a MAC adresa cílového zařízení se nastaví na *00:00:00:00:00:00*.

V Ethernet rámci se nastaví cílová MAC adresa na *ff:ff:ff:ff:ff:ff* a typ na 0x0806.

2.2 Skenování sítě

Pomocí IP adresy zdrojového zařízení a masky sítě získáme pomocí bitové operace logického součinu adresu sítě a z negace masky sítě a bitového logického součtu adresu broadcastu. První skenovaná adresa je o jedno vyšší jak adresa sítě a poslední o jedno nižší jak broadcast. Pro každou adresu se aktualizuje IP adresa cílového zařízení v ARP žádosti a odešle se. Po odeslání určitého bloku žádostí (zvoleno 20) se počká 1 sekundu na odpovědi a pokračuje se až do vyčerpání adres lokální sítě.

2.3 Formát výstupu

O výstup v požadovaném formátu se starají třídy `Devices`, `MAC` a `IP`. Třídy se také starají o přiřazení více IP adres k jedné MAC adrese, případně odstranění duplicit v obdržení více odpovědí od stejného zařízení.

3 Demonstrace

```
$ sudo ./ipk-scanner -i wlan0 -f ipk-scanner.xml
$ cat ./ipk-scanner.xml
<?xml version="1.0" encoding="UTF-8"?>
<devices>
   <host mac="0011.3262.4494">
      <ipv4>192.168.99.10</ipv4>
   </host>
   <host mac="d066.7b01.1cea">
      <ipv4>192.168.99.101</ipv4>
   </host>
   <host mac="e094.6747.0086">
      <ipv4>192.168.99.117</ipv4>
   </host>
   <host mac="44d9.e760.dadf">
      <ipv4>192.168.99.253</ipv4>
   </host>
</devices>
```

4 Reference

[1] Bouška, P.: TCP/IP - nalezení MAC adresy k IP - ARP. [online], cit. 2017-04-22.
URL http://www.samuraj-cz.com/clanek/tcpip-nalezeni-mac-adresy-k-ip-arp/

[2] Plummer, D. C.: RFC 826: An Ethernet Address Resolution Protocol. [online], cit. 2017-04-22.
URL https://tools.ietf.org/html/rfc826

[3] Wikipedie: Address Resolution Protocol. [online], cit. 2017-04-22.
URL https://cs.wikipedia.org/wiki/Address_Resolution_Protocol

[4] Wikipedie: Ethernet. [online], cit. 2017-04-22.
URL https://cs.wikipedia.org/wiki/Ethernet