

Přenos dat a počítačové sítě

Projekt 3

Obsah

Analýza síťového protokolu ARP/RARP	1
Zadání	1
Úplný text zadání	1
Můj paket.....	1
Obsah paketu	1
Popis struktury paketu	2
Přenosová vrstva Ethernet-u	2
Obsah Ethernet paketu.....	2
Dekódování paketu	3
Heuristika	3
Hlavička	3
Data	3
Literatura.....	5

Analýza síťového protokolu ARP/RARP

Zadání

Úplný text zadání

Protokol ARP (*Address Resolution Protocol*) je jednoduchý síťový protokol, který se používá při směrování k získání fyzické adresy počítače (*Ethernet Address*).

Úkolem je analyzovat zadaný paket:

- popsat jeho strukturu
- vysvětlit význam jednotlivých bitů (podle definice protokolu)
- určit, odkud kam byl paket poslán a za jakým účelem

Poznámky:

- při dekódování IP adres uveďte také doménovou adresu počítače (např. *eva.fit.vutbr.cz*), jestliže ji lze zjistit
- zadané pakety jsou uloženy v binární podobě na uvedené adrese (viz. soubor *los.pdf*). Rozdělení konkrétních úloh mezi studenty je zveřejněno tamtéž
- pro prohlížení paketů doporučujeme např. program *hexdump(1)* (*FreeBSD*)

Řešením projektu bude popsán rozbor paketu podle výše uvedených kritérií. V popisu uveďte význam všech bytů - nejlépe v hexadecimálním tvaru a jejich interpretaci podle protokolu. Zprávu odevzdejte ve formátu *pdf* nebo *ps* (*PostScript*) v češtině. Ve zprávě uveďte svoje pořadové číslo a číslo přiděleného paketu (obě informace jsou uvedeny v zadání - *pdf*).

Můj paket

Dokument s rozdělením paketů studentům (viz [R]) obsahuje následovní informace:

pořadí	příjmení	jméno	login	číslo paketu
162	Rozsnyó	Daniel	xrozs00	2

Obsah paketu

Dle zadání má můj paket číslo 2. Protože jeho obsah je ryze binární, není možné jeho přímé zobrazení ale použijeme hexadecimální výpis - vytvořený pomocí *BSD* utility *hexdump(1)*:

```
0000000 a000 96c9 6ad5 8000 f43f d510 0608 0100
0000010 0008 0406 0200 8000 f43f d510 e593 3608
0000020 a000 96c9 6ad5 e593 0c08
000002a
```

První sloupec je adresa (pozice v souboru) a zbytek jsou pak data - vždy 16 bajtů (128 bitů) na řádek. Pro snadnou čitelnost jsou ještě mezerou odděleny 2 bajty - 16 bitové slova.

Popis struktury paketu

Dokument [ARP] od organizace IETF (Internet Engineering Task Force) popisuje formát paketu ve své sekci *Packet Format* následovně:

Přenosová vrstva Ethernet-u

(nemusí nezbytně být přístupna uživateli, resp. vyšší vrstvě)

Počet bitů	Pole	Význam
48		Ethernet-ová adresa cíle
48		Ethernet-ová adresa odesílatele
16		Typ protokolu, konstantní hodnota: <i>ether_type\$ADDRESS_RESOLUTION</i>

Obsah Ethernet paketu

Počet bitů	Pole	Význam
16	<i>ar\$hdr</i>	Prostor adres zařízení (např. <i>Ethernet</i> , <i>Packet Radio</i>)
16	<i>ar\$pro</i>	Prostor adres protokolu, pro Ethernet je hodnota z množiny <i>ether_typ\$<protocol></i>
8	<i>ar\$hln</i>	délka každé adresy zařízení, v bajtech
8	<i>ar\$pln</i>	délka každé adresy protokolu, v bajtech
16	<i>ar\$op</i>	operační kód (<i>ares_op\$REQUEST</i> nebo <i>ares_op\$REPLY</i>)
n bajtů	<i>ar\$sha</i>	Adresa zařízení odesílatele (n je z pole <i>ar\$hln</i>)
m bajtů	<i>ar\$spa</i>	Adresa odesílatele v protokolu vyšší vrstvy (m je z <i>ar\$pln</i>)
n bajtů	<i>ar\$tha</i>	Adresa zařízení cíle (pokud je známa)
m bajtů	<i>ar\$tpa</i>	Adresa cíle v protokolu vyšší vrstvy

Dekódování paketu

Máme tyto vstupní data:

```
0000000 a000 96c9 6ad5 8000 f43f d510 0608 0100
0000010 0008 0406 0200 8000 f43f d510 e593 3608
0000020 a000 96c9 6ad5 e593 0c08
000002a
```

Protože nevíme jak byly pořízeny (na které vrstvě, jestli obsahují hlavičku nebo nikoliv), musíme se rozhodnout co budeme předpokládat. V podstatě máme dvě možnosti:

- předpokládat že paket obsahuje 1:1 to co popisuje ARP protokol (sekce výše)
- provést druh heuristické analýzy

Heuristika

Rozhodl jsem se pro druhou možnost (nejspíš protože lidi nejsou stroje, tudíž mají schopnost se vyvarovat chyb).

Ze svých zkušeností jako správce sítě vím, že v dnešní době se používá převážně ARP/RARP pro IPv4 nad Ethernet-em. Délky adres by teda měli obsahovat čísla jako 4 a 6. Čtyři je počet bajtů v 32 bitové IPv4 adrese a šest je analogicky počet bajtů v 48-bitové adrese Ethernet-ového zařízení (tj. MAC adresa). V paketu se nachází jedna z dvou kombinací (0406, 0604) zde:

```
0000000 a000 96c9 6ad5 8000 f43f d510 0608 0100
0000010 0008 0406 0200 8000 f43f d510 e593 3608
0000020 a000 96c9 6ad5 e593 0c08
```

Umístění je relativně v prostředku - a podle popisu struktury ARP, je to 5. a 6. bajt dat. Z tohoto můžeme již s jistotou usoudit že paket obsahuje i 14 bajtovou Ethernet-ovou hlavičku zde:

```
0000000 a000 96c9 6ad5 8000 f43f d510 0608 0100
0000010 0008 0406 0200 8000 f43f d510 e593 3608
0000020 a000 96c9 6ad5 e593 0c08
```

Hlavička

Poskytnete nám data o tom, z jakého na jaké zařízení putoval paket a co je to za paket:

```
0000000 a000 96c9 6ad5 8000 f43f d510 0608 0100 Cílová MAC
0000000 a000 96c9 6ad5 8000 f43f d510 0608 0100 Zdrojová MAC
0000000 a000 96c9 6ad5 8000 f43f d510 0608 0100 Typ paketu
```

V *Ethereal Wiki* [ERW] se lze dočíst o typech paketu/ typech protokolů - číslo které určuje jak se zpracují data z Ethernet-ového rámce (*frame*):

```
0x0806 ARP, Address Resolution Protocol
```

Hodnoty mají přehozené bajty, tudíž správné MAC adresy budou:

```
Odesílatel: 00-80-3F-F4-10-D5
Cíl: 00-A0-C9-96-D5-6A
```

Data

Datová složka rámce má při znalosti že jde o ARP paket následující význam (pozor na změnu pořadí v dvojicích bajtů):

```
0000000 a000 96c9 6ad5 8000 f43f d510 0608 0100 Zařízení
0000010 0008 0406 0200 8000 f43f d510 e593 3608 Protokol
0000010 0008 0406 0200 8000 f43f d510 e593 3608 4 bajtů - prot. adresa
0000010 0008 0406 0200 8000 f43f d510 e593 3608 6 bajtů - HW adresa
0000010 0008 0406 0200 8000 f43f d510 e593 3608 Operační kód
0000010 0008 0406 0200 8000 f43f d510 e593 3608 Odesílatel - HW
0000010 0008 0406 0200 8000 f43f d510 e593 3608 Odesílatel - protokol
0000020 a000 96c9 6ad5 e593 0c08 Cíl - HW
0000020 a000 96c9 6ad5 e593 0c08 Cíl - protokol
```

Zjištěné údaje jsou (po správné konverzi mezi *little-endian* a *big-endian*):

```
Druh zařízení:          0001
Druh protokolu:         0800
Adresa zařízení má délku: 06
Protokolová adresa má délku: 04
Operační kód protokolu ARP: 0002
```

Druh zařízení můžeme jednoznačně identifikovat pomocí komentovaného zdrojového kódu k Linux-ovému jádru jako *Ethernet* - konkrétně v souboru *include/linux/if_arp.h* je:

```
/* ARP protocol HARDWARE identifiers. */
#define ARPHRD_ETHER 1 /* Ethernet 10Mbps */
```

Druh protokolu bude IP (*Internet Protocol*), protože jsme našli hodnotu 0800, která zodpovídá právě tomuto protokolu. Jako zdroj posloužil tentokrát soubor *include/linux/if_ether.h*:

```
/*
 * These are the defined Ethernet Protocol ID's.
 */
#define ETH_P_IP 0x0800 /* Internet Protocol packet */
```

Operační kód má hodnotu 2 což je operace REPLY, tj. odpověď na ARP dotaz. K dekodování nám opět pomůže soubor *if_arp.h* ve kterém jsou operace definovány následovně:

```
/* ARP protocol opcodes. */
#define ARPOP_REQUEST 1 /* ARP request */
#define ARPOP_REPLY 2 /* ARP reply */
#define ARPOP_RREQUEST 3 /* RARP request */
#define ARPOP_RREPLY 4 /* RARP reply */
```

Délky adres - nám určili kolik bajtů mají adresy, které jsou (v notaci pro MAC a IPv4):

```
Odesílatel:
- adresa zařízení:      00-80-3F-F4-10-D5
- adresa protokolu:     93.E5.08.36
Cíl:
- adresa zařízení:     00-A0-C9-96-D5-6A
- adresa protokolu:     93.E5.08.0C
```

Adresy zařízení - nejsou velmi podstatné, můžeme říct o strojích můžeme říct jen tolik že velice pravděpodobně mají síťové karty od různých výrobců, z evidence *IEEE* [OUI] zjistíme výrobce:

```
00-80-3F (hex) TATUNG COMPANY
00-A0-C9 (hex) INTEL CORPORATION - HF1-06
```

Adresy protokolu - protože normálně používáme dekadický zápis, můžeme adresy převést:

```
Odesílatel: 93.E5.08.36 = 147.229.8.54
Cíl:        93.E5.08.0C = 147.229.8.12
```

Číselné IP adresy se pak můžou převést na reverzní DNS záznamy třeba pomocí příkazu *nslookup(1)*, z našich adres dostáváme

```
Odesílatel: 147.229.8.54 -> bivoj.fit.vutbr.cz
Cíl:        147.229.8.12 -> kazi.fit.vutbr.cz
```

Smyslem paketu bylo říct serveru s IP adresou 147.229.8.12 (tj. *kazi.fit.vutbr.cz*), že stroj s IP adresou 147.229.8.54 (tj. *bivoj.fit.vutbr.cz*) má MAC adresu 00-80-3F-F4-10-D5. Širší kontext komunikace je že server *kazi* chtěl komunikovat se strojem *bivoj*, takže se ho zeptal jakou má MAC adresu, načež mu ten stroj odpověděl výše rozebíraným paketem.

Pokud by jsme předpokládali na začátku, že paket je 1:1 to co popisuje RFC dokumentace, tak bychom nemuseli odhalit přehození bajtů, ale v podstatě by jsme se dopracovali k stejnému výsledku.

Literatura

- [R] **Rozdělení arp paketů jednotlivým studentům**
<https://www.fit.vutbr.cz/study/courses/PDT/private/projekty/2004/los.pdf>
- [ARP] **RFC 826: An Ethernet Address Resolution Protocol**
Network Working Group, David C. Plummer, November 1982
<http://ietf.org/rfc/rfc0826.txt>
- [ERW] **Ethernet - The Ethereal Wiki**
<http://wiki.ethereal.com/Ethernet>
- [LK] **Global definitions for the ARP (RFC 826) protocol**
Linux Kernel source, soubory `include/linux/if_arp.h` a `include/linux/if_ether.h`
<http://kernel.org>
- [OUI] **IEEE OUI and Company_id Assignments**
<http://standards.ieee.org/regauth/oui/oui.txt>