

LV02_Osnovna analiza mrežnog prometa

PRIPREMA ZA VJEŽBU

U pisanoj formi odgovori na slijedeća pitanja:

1. Što je i čemu služi protokol ARP?

- Protokol koji služi za mapiranje IP adresa na fizičke MAC adrese

2. Što je i čemu služi protokol ICMP?

- Komunikacijski protokol, omogućuje mrežnim prolazima ili računalima slanje kontrolnih poruka o greškama

3. Što znaš o naredbi ping?

- Administrativni alat koji služi za provjeru dostupnosti poslužitelja na računalnim mrežama

IZVOĐENJE VJEŽBE

- Pokrenuti program za praćenje protokola Wireshark
- Odabrati mrežnu karticu na kojoj će se pratiti promet podataka
- Pokrenuti praćenje prometa na mrežnoj kartici

1.Zadatak

Lan kabelom povežemo 2 računala.

2.Zadatak

Internet Protocol Version 4 (TCP/IPv4) Properties

General

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

Obtain an IP address automatically

Use the following IP address:

IP address:	192 . 168 . 10 . 2
Subnet mask:	255 . 255 . 255 . 0
Default gateway:	. . .

Obtain DNS server address automatically

Use the following DNS server addresses:

Preferred DNS server:	. . .
Alternate DNS server:	. . .

Validate settings upon exit

Advanced...

OK Cancel

3. zadatak

Pokrenuti program Wireshark.

Pričekati da se prikaže prvih dvadesetak redaka, a onda zaustaviti hvatanje (Capture – Stop).

a) Koliko je točno okvira Wireshark „uhvatio“?

- 20

b) Koje su oznake protokola na tim okvirima?

- LLMNR, NBNS, MDNS, ARP

Time	Source	Destination	Protocol	Length
1 0.000000	192.168.10.3	192.168.10.255	NBNS	
2 0.295431	AsrockIn_d4:aa:2d	Broadcast	ARP	
3 0.483937	192.168.10.3	192.168.10.255	NBNS	
4 0.484338	192.168.10.3	224.0.0.251	MDNS	
5 0.484630	fe80::3020:de3e:b87...	ff02::fb	MDNS	
6 0.485235	fe80::3020:de3e:b87...	ff02::1:3	LLMNR	
7 0.485519	192.168.10.3	224.0.0.252	LLMNR	
8 0.905142	fe80::3020:de3e:b87...	ff02::1:3	LLMNR	
9 0.905485	192.168.10.3	224.0.0.252	LLMNR	
10 1.248444	192.168.10.3	192.168.10.255	NBNS	
11 1.326557	AsrockIn_d4:aa:2d	Broadcast	ARP	
12 1.483748	192.168.10.3	224.0.0.251	MDNS	
13 1.484067	fe80::3020:de3e:b87...	ff02::fb	MDNS	
14 1.999260	192.168.10.3	192.168.10.255	NBNS	
15 2.295345	AsrockIn_d4:aa:2d	Broadcast	ARP	
16 2.475886	192.168.10.3	192.168.10.255	NBNS	
17 2.476325	192.168.10.3	224.0.0.251	MDNS	
18 2.476615	fe80::3020:de3e:b87...	ff02::fb	MDNS	
19 2.477326	fe80::3020:de3e:b87...	ff02::1:3	LLMNR	
20 2.477622	192.168.10.3	224.0.0.252	LLMNR	

c) Koristeći dostupne informacije sa predavanja/Interneta opiši kratko funkcije tih protokola.

- LLMNR: Omogućuje IPv4 i IPv6 hostovima da izvrše, razrješe imena za hostove na istoj lokalnoj vezi

- NBNS: Protokol za razlučivanje imena

- MDNS: Protokol koji razrješava imena hostova u IP adrese unutar malih mreža gdje lokalni poslužitelj nije uključen

- ARP: Protokol koji povezuje stalno promijenjivu adresu IP s fiksnom fizičkom adresom

d) Analiziraj okvir koji u sebi nosi:

ARP paket (protokol) request te ispiši:

- polazišnu MAC adresu

70:85:c2:ce:9b:92

- odredišnu MAC adresu

ff:ff:ff:ff:ff:ff

- polazišnu IP adresu

192.168.10.2

- odredišnu IP adresu

192.168.10.1

ARP paket (protokol) – reply te ispiši:

- polazišnu MAC adresu

70:85:c2:ce:9b:92

- odredišnu MAC adresu

ff:ff:ff:ff:ff:ff

- Kolika je veličina svake od ovih adresa?

0x00000806

- polazišnu IP adresu

192.168.10.2

- odredišnu IP adresu

192.168.10.3

e) Kako glasi odredišna MAC adresa prvog Ethernet okvira kod ARP protokola i zašto?

ff:ff:ff:ff:ff:ff, zato što je to broadcast adresa i šalje se svima

4. zadatak

U istom spoju računala pomoću Wiresharka analiziraj ICMP promet korištenjem naredbe ping sa jednog računala na drugo.

a) Koliko je ICMP echo i reply paketa?

```
Internet Control Message Protocol
  Type: 8 (Echo (ping) request)
  Code: 0
  Checksum: 0x4d56 [correct]
  [Checksum Status: Good]
  Identifier (BE): 1 (0x0001)
  Identifier (LE): 256 (0x0100)
  Sequence number (BE): 5 (0x0005)
  Sequence number (LE): 1280 (0x0500)
  [Response frame: 18]
```

b) Koji protokol pokreće naredba ping?

-ICMP

c) Sastavni dio kojeg protokola je ICMP protokol?

-IP

d) U koji okvir je enkapsuliran IP paket?

Time	Source	Destination	Protocol	Length	Info
17.2.027649	192.168.10.2	192.168.10.3	ICMP	74	Echo (ping) request id=0x0001, seq=5/1280, ttl=128 (reply in 18)

Izaberi jedan redak koji se odnosi na protokol ICMP, ispiši njegov sadržaj te odgovori na slijedeća pitanja:

e) Koja je polazišna IP adresa?

192.168.10.2

f) Koja je odredišna IP adresa?

192.168.10.3

g) Koja je MAC adresa polazišnog uređaja?

70:85:c2:ce:9b:92

h) Koja je MAC adresa odredišnog uređaja?

70:85:c2:d4:aa:2d

i) Koja je oznaka vrste podataka u Ethernet okviru?

```
> Frame 17: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface e
▼ Ethernet II, Src: AsrockIn_ce:9b:92 (70:85:c2:ce:9b:92), Dst: AsrockIn_d4:aa:2d (70:85:c2:d4:aa:2d)
  > Destination: AsrockIn_d4:aa:2d (70:85:c2:d4:aa:2d)
  > Source: AsrockIn_ce:9b:92 (70:85:c2:ce:9b:92)
  Type: IPv4 (0x0800)
▼ Internet Protocol Version 4, Src: 192.168.10.2, Dst: 192.168.10.3
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
  Total Length: 60
  Identification: 0x0445 (1093)
  > Flags: 0x0000
  Time to live: 128
  Protocol: ICMP (1)
  Header checksum: 0xa126 [validation disabled]
  [Header checksum status: Unverified]
  Source: 192.168.10.2
  Destination: 192.168.10.3
▼ Internet Control Message Protocol
```

j) Koja je veličina IP adrese, a koja MAC adrese u okvirima/paketima?

IP adresa: 60 bitova

MAC adresa: 48 bitova

k) Koja je veličina IP paketa kod ICMP protokola?

60 bitova

l) Koja je veličina podataka u IP paketu kod ICMP protokola?

20 bitova

m) Postavi filter da se prati samo ICMP protokol.

	Time	Source	Destination	Protocol	Length
17	2.027649	192.168.10.2	192.168.10.3	ICMP	7
18	2.027862	192.168.10.3	192.168.10.2	ICMP	7
25	3.039646	192.168.10.2	192.168.10.3	ICMP	7
26	3.039882	192.168.10.3	192.168.10.2	ICMP	7
29	4.047285	192.168.10.2	192.168.10.3	ICMP	7
30	4.047586	192.168.10.3	192.168.10.2	ICMP	7
32	5.062017	192.168.10.2	192.168.10.3	ICMP	7
33	5.062320	192.168.10.3	192.168.10.2	ICMP	7

n) Koliko je ICMP echo i reply paketa?

```
Internet Control Message Protocol
  Type: 8 (Echo (ping) request)
  Code: 0
  Checksum: 0x4d56 [correct]
  [Checksum Status: Good]
  Identifier (BE): 1 (0x0001)
  Identifier (LE): 256 (0x0100)
  Sequence number (BE): 5 (0x0005)
  Sequence number (LE): 1280 (0x0500)
  [Response frame: 18]
```

o) Koji protokol pokreće naredba ping?

-ICMP

p) Sastavni dio kojeg protokola je protokol ICMP?

-IP

q) U koji okvir je enkapsuliran IP paket?

Time	Source	Destination	Protocol	Length	Info
17	2.027649	192.168.10.2	192.168.10.3	ICMP	74 Echo (ping) request id=0x0001, seq=5/1280, ttl=128 (reply in 18)

5. Zadatak

Računala ponovno spojiti u školsku mrežu i provjeriti mrežne postavke.