

Tehnička škola Ruđera Boškovića
Zagreb, Getaldićeva 4

Niko Josipović
Osnovna analiza mrežnog prometa
LABORATORIJSKA VJEŽBA

Zagreb, listopad 2024.

CILJ VJEŽBE

Učenik će znati samostalno pratiti i napraviti osnovnu analizu prometa na vezi.

PRIPREMA ZA VJEŽBU

1. Što je i čemu služi protokol ARP?

- ARP (Address Resolution Protocol) je komunikacijski protokol kojim se povezuje IP adresa i fiksna fizička adresa nekog uređaja na lokalnoj mreži (LAN) poznata pod nazivom MAC. Iz logičke (IP) adrese se dobiva fizička (MAC) adresa.

2. Što je i čemu služi protokol ICMP?

- ICMP je komunikacijski protokol koji je ugrađen u svaki IP modul kako bi usmjerinicima ili računalima omogućio slanje kontrolnih poruka o greškama. Uloga ICMP je prijavljivanje grešaka, u komunikaciji, **bez njihovog ispravljanja**.

3. Što znaš o naredbi ping?

- Ping je osnovni mrežni alat koji služi za provjeru dostupnosti određenog hosta povezanog u IP mrežu. To postiže slanjem paketa sa ICMP porukom prema određenom računalu. Šalje se paket echo request, a iščekuje ICMP echo response.

IZVOĐENJE VJEŽBE

1. Povezati dva susjedna računala u P2P spoj.



2. Konfigurirati računala za rad u mreži, prema tablici:

Oznaka na shemi	PC1	PC2
Naziv radne stanice	WSx	WSy
IP adresa	192.168.10.2	192.168.10.3
Subnet maska	255.255.255.0	255.255.255.0
Default Gateway	192.168.10.1	192.168.10.1

IP settings

IP assignment:	Manual
IPv4 address:	192.168.10.3
IPv4 subnet prefix length:	24
IPv4 gateway:	192.168.10.1

Edit

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

a) Koliko je točno okvira Wireshark „uhvatio“?

- 20 okvir

1	0.000000	MicroStarINT_c7:52:...	Broadcast	ARP	42	Who has 192.168.10.1? Tell 192.168.10.3
2	2.031358	MicroStarINT_c7:52:...	Broadcast	ARP	42	Who has 192.168.10.1? Tell 192.168.10.3
3	2.998668	MicroStarINT_c7:52:...	Broadcast	ARP	42	Who has 192.168.10.1? Tell 192.168.10.3
4	4.003992	MicroStarINT_c7:52:...	Broadcast	ARP	42	Who has 192.168.10.1? Tell 192.168.10.3
5	5.004305	MicroStarINT_c7:52:...	Broadcast	ARP	42	Who has 192.168.10.1? Tell 192.168.10.3
6	6.011112	MicroStarINT_c7:52:...	Broadcast	ARP	42	Who has 192.168.10.1? Tell 192.168.10.3
7	18.078043	MicroStarINT_c7:52:...	Broadcast	ARP	60	Who has 192.168.10.1? Tell 192.168.10.2
8	18.704461	MicroStarINT_c7:52:...	Broadcast	ARP	60	Who has 192.168.10.1? Tell 192.168.10.2
9	19.710168	MicroStarINT_c7:52:...	Broadcast	ARP	60	Who has 192.168.10.1? Tell 192.168.10.2
10	27.850762	MicroStarINT_c7:52:...	Broadcast	ARP	60	Who has 192.168.10.1? Tell 192.168.10.2
11	28.708045	MicroStarINT_c7:52:...	Broadcast	ARP	60	Who has 192.168.10.1? Tell 192.168.10.2
12	29.708062	MicroStarINT_c7:52:...	Broadcast	ARP	60	Who has 192.168.10.1? Tell 192.168.10.2
13	36.251758	MicroStarINT_c7:52:...	Broadcast	ARP	60	Who has 192.168.10.1? Tell 192.168.10.2
14	37.197230	MicroStarINT_c7:52:...	Broadcast	ARP	60	Who has 192.168.10.1? Tell 192.168.10.2
15	38.202708	MicroStarINT_c7:52:...	Broadcast	ARP	60	Who has 192.168.10.1? Tell 192.168.10.2
16	43.879028	MicroStarINT_c7:52:...	Broadcast	ARP	42	Who has 192.168.10.1? Tell 192.168.10.3
17	44.500679	MicroStarINT_c7:52:...	Broadcast	ARP	42	Who has 192.168.10.1? Tell 192.168.10.3
18	45.497311	MicroStarINT_c7:52:...	Broadcast	ARP	42	Who has 192.168.10.1? Tell 192.168.10.3
19	67.877016	MicroStarINT_c7:52:...	Broadcast	ARP	42	Who has 192.168.10.1? Tell 192.168.10.3
20	68.497310	MicroStarINT_c7:52:...	Broadcast	ARP	42	Who has 192.168.10.1? Tell 192.168.10.3

b) Koje su oznake protokola na tim okvirima?

- ARP protokol

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

- ARP je komunikacijski protokol kojim se povezuje IP adresa i fiksna fizička adresa nekog uređaja na lokalnoj mreži (LAN) poznata pod nazivom MAC. Iz logičke (IP) adrese se dobiva fizička (MAC) adresa

d) Analiziraj okvir koji u sebi nosi:

ARP paket (protokol) request te ispiši:

```
Frame 7: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface \Device\NPF_{83B7F...}
Ethernet II, Src: MicroStarINT_c7:52:c3 (04:7c:16:c7:52:c3), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
  Destination: Broadcast (ff:ff:ff:ff:ff:ff)
  Source: MicroStarINT_c7:52:c3 (04:7c:16:c7:52:c3)
  Type: ARP (0x0806)
  [Stream index: 2]
Address Resolution Protocol (request)
  Hardware type: Ethernet (1)
  Protocol type: IPv4 (0x0800)
  Hardware size: 6
  Protocol size: 4
  Opcode: request (1)
  Sender MAC address: MicroStarINT_c7:52:c3 (04:7c:16:c7:52:c3)
  Sender IP address: 192.168.10.3
  Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)
  Target IP address: 192.168.10.1
```

- polazišnu MAC adresu: **04:7c:16:c7:52:c3**
- odredišnu MAC adresu: **ff:ff:ff:ff:ff:ff (broadcast)**
- polazišnu IP adresu: **192.168.10.3**
- odredišnu IP adresu: **192.168.10.1**

ARP paket (protokol) reply te ispiši:

```
▶ Frame 58: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface \Device\NPF_{83B...}
▶ Ethernet II, Src: MicroStarINT_c7:52:da (04:7c:16:c7:52:da), Dst: MicroStarINT_c7:52:c3 (04:7c:16...
▼ Address Resolution Protocol (reply)
  Hardware type: Ethernet (1)
  Protocol type: IPv4 (0x0800)
  Hardware size: 6
  Protocol size: 4
  Opcode: reply (2)
  Sender MAC address: MicroStarINT_c7:52:da (04:7c:16:c7:52:da)
  Sender IP address: 192.168.10.2
  Target MAC address: MicroStarINT_c7:52:c3 (04:7c:16:c7:52:c3)
  Target IP address: 192.168.10.3
```

- polazišnu MAC adresu: **04:7c:16:c7:52:da**
 - odredišnu MAC adresu: **04:7c:16:c7:52:c3**
 - Kolika je veličina svake od ovih adresa? **6 bajta**
 - polazišnu IP adresu: **192.168.10.2**
 - odredišnu IP adresu: **192.168.10.3**
4. 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?

- Ima **osam** ICMP echo i reply paketa

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.10.3	192.168.10.2	ICMP	74	Echo (ping) request
2	0.000536	192.168.10.2	192.168.10.3	ICMP	74	Echo (ping) reply
3	1.005244	192.168.10.3	192.168.10.2	ICMP	74	Echo (ping) request
4	1.005716	192.168.10.2	192.168.10.3	ICMP	74	Echo (ping) reply
5	2.015927	192.168.10.3	192.168.10.2	ICMP	74	Echo (ping) request
6	2.016356	192.168.10.2	192.168.10.3	ICMP	74	Echo (ping) reply
7	3.035222	192.168.10.3	192.168.10.2	ICMP	74	Echo (ping) request
8	3.035731	192.168.10.2	192.168.10.3	ICMP	74	Echo (ping) reply

- b) Koji protokol pokreće naredba ping?

- ICMP

- c) Koji protokol pokreće naredba ping?

- IP protokol

- d) Koji protokol pokreće naredba ping?

- Enkapsuliran u Ethernet II. Paket

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

- e) Koja je polazišna IP adresa?

- Polazišna IP adresa: 192.168.10.2

- f) Koja je odredišna IP adresa?

- Odredišna IP adresa: 192.168.10.3

- g) Koja je MAC adresa polazišnog uređaja?

- 04:7c:16:c7:52:c3

h) Koja je MAC adresa odredišnog uređaja?

- 04:7c:16:c7:52:da

i) Koja je oznaka vrste podataka u Ethernet okviru?

```
▼ Ethernet II, Src: MicroStarINT_c7:52:c3 (04:7c:16:c7:52:c3), Dst: MicroStarINT_c7:52:da (04:7c:16:c7:52:da)
  ▼ Destination: MicroStarINT_c7:52:da (04:7c:16:c7:52:da)
    ....0. .... = LG bit: Globally unique address (factory default)
    ....0. .... = IG bit: Individual address (unicast)
  ▼ Source: MicroStarINT_c7:52:c3 (04:7c:16:c7:52:c3)
    ....0. .... = LG bit: Globally unique address (factory default)
    ....0. .... = IG bit: Individual address (unicast)
  Type: IPv4 (0x0800)
  [Stream index: 0]
```

- Vrsta podataka: Ipv4 (0x0800)

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

- IP adrese je 4 bajta, a MAC adrese 6 bajta

k) Koja je veličina IP paketa kod ICMP protokola?

- 60 bajta („Total length“)

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

- 40 bajta -> „Total length“ - „Header length“

m) Postavi filter da se prati samo ICMP protokol.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.10.3	192.168.10.2	ICMP	74	Echo (ping) request id=0x0001, seq=13/3328, ttl=128 (reply in 2)
2	0.000531	192.168.10.2	192.168.10.3	ICMP	74	Echo (ping) reply id=0x0001, seq=13/3328, ttl=128 (request in 1)
3	1.005347	192.168.10.3	192.168.10.2	ICMP	74	Echo (ping) request id=0x0001, seq=14/3584, ttl=128 (reply in 4)
4	1.005855	192.168.10.2	192.168.10.3	ICMP	74	Echo (ping) reply id=0x0001, seq=14/3584, ttl=128 (request in 3)
5	2.030050	192.168.10.3	192.168.10.2	ICMP	74	Echo (ping) request id=0x0001, seq=15/3840, ttl=128 (reply in 6)
6	2.030572	192.168.10.2	192.168.10.3	ICMP	74	Echo (ping) reply id=0x0001, seq=15/3840, ttl=128 (request in 5)
7	3.052994	192.168.10.3	192.168.10.2	ICMP	74	Echo (ping) request id=0x0001, seq=16/4096, ttl=128 (reply in 8)
8	3.053529	192.168.10.2	192.168.10.3	ICMP	74	Echo (ping) reply id=0x0001, seq=16/4096, ttl=128 (request in 7)

5. Računala ponovno spojiti u školsku mrežu i provjeriti mrežne postavke. Učitati tri web stranice i pratiti promet na vezi pomoću alata Wireshark računala na drugo.

6484	25.290782	192.168.123.14	193.198.184.130	DNS	85	Standard query 0x1099 HTTPS chrome.cloudflare-dns.com
6485	25.291183	192.168.123.14	193.198.184.130	DNS	80	Standard query 0x3959 A tunnel.googlezip.net
6486	25.292426	193.198.184.130	192.168.123.14	DNS	158	Standard query response 0x1099 HTTPS chrome.cloudflare
6487	25.292426	193.198.184.130	192.168.123.14	DNS	117	Standard query response 0xe15b A chrome.cloudflare-dns
6488	25.292791	193.198.184.130	192.168.123.14	DNS	96	Standard query response 0x3959 A tunnel.googlezip.net
3715	7.821554	192.168.123.14	161.53.160.228	HTTP	587	GET /favicon.ico/ HTTP/1.1
3724	8.104438	161.53.160.228	192.168.123.14	HTTP	1514	[TCP Previous segment not captured] Continuation
3726	8.104438	161.53.160.228	192.168.123.14	HTTP	1514	Continuation
3727	8.104438	161.53.160.228	192.168.123.14	HTTP	1514	Continuation
3733	8.104763	161.53.160.228	192.168.123.14	HTTP	1514	Continuation
3734	8.104763	161.53.160.228	192.168.123.14	HTTP	1514	Continuation
3736	8.104763	161.53.160.228	192.168.123.14	HTTP	1514	Continuation
3737	8.104763	161.53.160.228	192.168.123.14	HTTP	1266	Continuation
5075	14.185216	192.168.123.14	161.53.160.228	HTTP	630	GET / HTTP/1.1
5594	14.442488	161.53.160.228	192.168.123.14	HTTP	1514	[TCP Previous segment not captured] Continuation
5596	14.442488	161.53.160.228	192.168.123.14	HTTP	1514	Continuation
5598	14.442488	161.53.160.228	192.168.123.14	HTTP	1514	Continuation
5599	14.442488	161.53.160.228	192.168.123.14	HTTP	1514	Continuation
5600	14.442488	161.53.160.228	192.168.123.14	HTTP	1514	Continuation
5606	14.442969	161.53.160.228	192.168.123.14	HTTP	1514	Continuation
5607	14.442969	161.53.160.228	192.168.123.14	HTTP	1514	Continuation
5608	14.442969	161.53.160.228	192.168.123.14	HTTP	1266	Continuation