# LV2: Osnovna analiza mrežnog prometa

## Bruno Tolić Kalanj, Marin Šupljika 3.c

### PRIPREMA ZA VJEŽBU

U pisanoj formi odgovori na slijedeća pitanja:

1. **Što je i čemu služi protokol ARP?**
   ARP (Address Resolution Protocol) je mrežni protokol koji se koristi za prevođenje IP adresa u fizičke adrese (MAC adrese). Na lokalnoj mreži, kada jedno računalo želi komunicirati s drugim, koristi ARP kako bi saznalo MAC adresu uređaja kojem šalje podatke na osnovu njegove IP adrese.

2. **Što je i čemu služi protokol ICMP?**
   ICMP (Internet Control Message Protocol) koristi se za slanje dijagnostičkih poruka o stanju mreže, kao što su obavijesti o greškama ili informacije o neuspjehu isporuke paketa. Koristi se u alatima poput "ping" za testiranje mrežne povezanosti i otkrivanje kašnjenja ili gubitaka u mreži.

3. **Što znaš o naredbi ping?**
   Ping je mrežni alat koji koristi ICMP protokol za slanje ICMP echo request poruka na drugo računalo i očekuje ICMP echo reply poruke natrag. Ova naredba se koristi za provjeru je li uređaj dostupan u mreži i za mjerenje vremena koje je potrebno da paket stigne do odredišta i natrag (round-trip time - RTT).

### IZVOĐENJE VJEŽBE

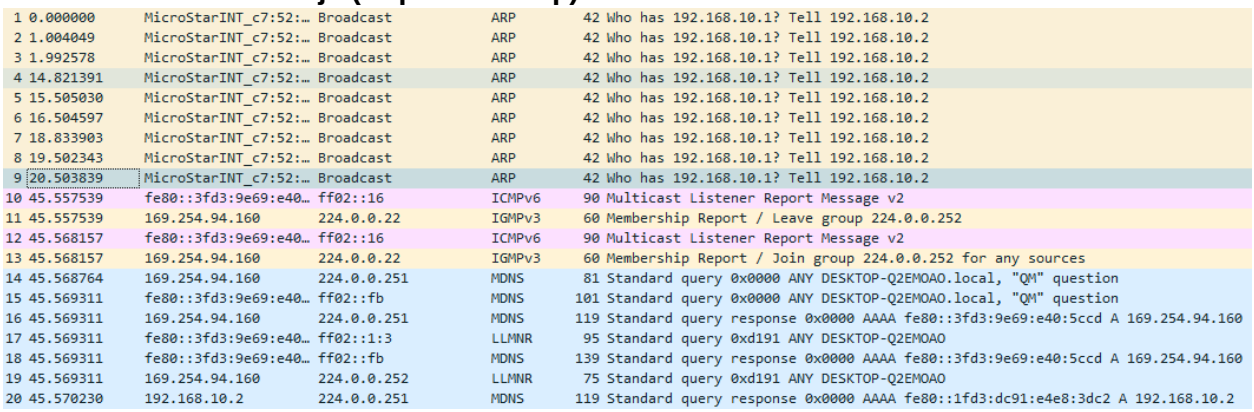
- **Pokrenuti program za praćenje protokola Wireshark**
- **Odabrati mrežnu karticu na kojoj će se pratiti promet podataka**
- **Pokrenuti praćenje prometa na mrežnoj kartici**

1. **Povezati dva susjedna računala odgovarajućim kabelom te uspostaviti P2P spoj. Topologija:**

2. **Konfigurirati računala za rad u mreži, pri čemu koristiti adresnu shemu 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 |

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



| | | | | | |
|---|---|---|---|---|---|
| 1 | 0.000000 | MicroStarINT_c7:52:… | Broadcast | ARP | 42 Who has 192.168.10.1? Tell 192.168.10.2 |
| 2 | 1.004049 | MicroStarINT_c7:52:… | Broadcast | ARP | 42 Who has 192.168.10.1? Tell 192.168.10.2 |
| 3 | 1.992578 | MicroStarINT_c7:52:… | Broadcast | ARP | 42 Who has 192.168.10.1? Tell 192.168.10.2 |
| 4 | 14.821391 | MicroStarINT_c7:52:… | Broadcast | ARP | 42 Who has 192.168.10.1? Tell 192.168.10.2 |
| 5 | 15.505030 | MicroStarINT_c7:52:… | Broadcast | ARP | 42 Who has 192.168.10.1? Tell 192.168.10.2 |
| 6 | 16.504597 | MicroStarINT_c7:52:… | Broadcast | ARP | 42 Who has 192.168.10.1? Tell 192.168.10.2 |
| 7 | 18.833903 | MicroStarINT_c7:52:… | Broadcast | ARP | 42 Who has 192.168.10.1? Tell 192.168.10.2 |
| 8 | 19.502343 | MicroStarINT_c7:52:… | Broadcast | ARP | 42 Who has 192.168.10.1? Tell 192.168.10.2 |
| 9 | 20.503839 | MicroStarINT_c7:52:… | Broadcast | ARP | 42 Who has 192.168.10.1? Tell 192.168.10.2 |
| 10 | 45.557539 | fe80::3fd3:9e69:e40… | ff02::16 | ICMPv6 | 90 Multicast Listener Report Message v2 |
| 11 | 45.557539 | 169.254.94.160 | 224.0.0.22 | IGMPv3 | 60 Membership Report / Leave group 224.0.0.252 |
| 12 | 45.568157 | fe80::3fd3:9e69:e40… | ff02::16 | ICMPv6 | 90 Multicast Listener Report Message v2 |
| 13 | 45.568157 | 169.254.94.160 | 224.0.0.22 | IGMPv3 | 60 Membership Report / Join group 224.0.0.252 for any sources |
| 14 | 45.568764 | 169.254.94.160 | 224.0.0.251 | MDNS | 81 Standard query 0x0000 ANY DESKTOP-Q2EMOAO.local, "QM" question |
| 15 | 45.569311 | fe80::3fd3:9e69:e40… | ff02::fb | MDNS | 101 Standard query 0x0000 ANY DESKTOP-Q2EMOAO.local, "QM" question |
| 16 | 45.569311 | 169.254.94.160 | 224.0.0.251 | MDNS | 119 Standard query response 0x0000 AAAA fe80::3fd3:9e69:e40:5ccd A 169.254.94.160 |
| 17 | 45.569311 | fe80::3fd3:9e69:e40… | ff02::1:3 | LLMNR | 95 Standard query 0xd191 ANY DESKTOP-Q2EMOAO |
| 18 | 45.569311 | fe80::3fd3:9e69:e40… | ff02::fb | MDNS | 139 Standard query response 0x0000 AAAA fe80::3fd3:9e69:e40:5ccd A 169.254.94.160 |
| 19 | 45.569311 | 169.254.94.160 | 224.0.0.252 | LLMNR | 75 Standard query 0xd191 ANY DESKTOP-Q2EMOAO |
| 20 | 45.570230 | 192.168.10.2 | 224.0.0.251 | MDNS | 119 Standard query response 0x0000 AAAA fe80::1fd3:dc91:e4e8:3dc2 A 192.168.10.2 |

a) **Koliko je točno okvira Wireshark „uhvatio“?**
   20
b) **Koje su oznake protokola na tim okvirima?**
   ARP,ICMP,MDNS,LLMNR i IGMP
c) **Koristeći dostupne informacije sa predavanja/Interneta opiši kratko funkcije tih protokola.**
   ARP (Address Resolution Protocol) je mrežni protokol koji se koristi za prevođenje IP adresa u fizičke adrese (MAC adrese)
   ICMP (Internet Control Message Protocol) koristi se za slanje dijagnostičkih poruka o stanju mreže, kao što su obavijesti o greškama ili informacije o neuspjehu isporuke paketa

**d) Analiziraj okvir koji u sebi nosi:**
**ARP paket (protokol) request te ispiši:**
**- polazišnu MAC adresu**

`04:7c:16:c7:52:f1`

**- odredišnu MAC adresu**

`Broadcast (ff:ff:ff:ff:ff:ff)` **- polazišnu IP adresu**

192.168.10.2
**- odredišnu IP adresu**
192.168.10.3

**ARP paket (protokol) – reply te ispiši:**
**- polazišnu MAC adresu**

```
39 150.303334    MicroStarINT_c7:52:… MicroStarINT_c7:53:… ARP        42 192.168.10.2 is at 04:7c:16:c7:52:f1
```

**- odredišnu MAC adresu**

```
37 150.258534    MicroStarINT_c7:53:… MicroStarINT_c7:52:… ARP        60 192.168.10.3 is at 04:7c:16:c7:53:2a
```

**- Kolika je veličina svake od ovih adresa?**
60 byts
**- polazišnu IP adresu - odredišnu IP adresu**

```
Sender MAC address: MicroStarINT_c7:53:2a (04:7c:16:c7:53:2a)
Sender IP address: 192.168.10.3
Target MAC address: MicroStarINT_c7:52:f1 (04:7c:16:c7:52:f1)
Target IP address: 192.168.10.2
```

**d) Kako glasi odredišna MAC adresa prvog Ethernet okvira kod ARP protokola i zašto?**
MAC adresa odretišta prvog ARP requesta je broadcast adresa koja ima vrijednost ff:ff:ff:ff:ff. Razlog tome je taj što pošiljatelj ne zna MAC adresu odredišnog uređaja i želi poslati ARP upit svim računalima u mreži.

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?**
   4 echo i 4 reply
   b) **Koji protokol pokreće naredba ping?**
   ICMP
   c) **Sastavni dio kojeg protokola je ICMP protokol?**
   ICMP je sastavni dio **IP** (Internet Protocol) paketa, koji se koristi za mrežnu komunikaciju na mrežnom sloju.
   d) **U koji okvir je enkapsuliran IP paket?**
   IP paket je enkapsuliran unutar **Ethernet** okvira kada se koristi Ethernet mreža za komunikaciju.

**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 3 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 (PC1)
**f) Koja je odredišna IP adresa?**
192.168.10.3 (PC2)
**g) Koja je MAC adresa polazišnog uređaja?**
MAC adresa računala s kojeg se šalje ping. U Wiresharku u okviru za Ethernet, označena kao Source MAC Address.
**h) Koja je MAC adresa odredišnog uređaja?**
MAC adresa računala kojem šaljemo ping, označena kao Destination MAC Address.

**i) Koja je oznaka vrste podataka u Ethernet okviru?**
Oznaka vrste podataka u Ethernet okviru je 0x0800, što označava da je sadržaj okvira IPv4 paket.
**j) Koja je veličina IP adrese, a koja MAC adrese u okvirima/paketima?**
IP adresa je veličine 4 bajta (32 bita) u IPv4.
MAC adresa je veličine 6 bajta (48 bita).
**k) Koja je veličina IP paketa kod ICMP protokola?**
Veličina IP paketa može varirati, ali minimalna veličina je 20 bajta za IP zaglavlje, plus veličina ICMP poruke. ICMP echo request/reply poruka je obično 8 bajta, pa je minimalna ukupna veličina IP paketa oko 28 bajta.
**l) Koja je veličina podataka u IP paketu kod ICMP protokola?**
Veličina podataka može varirati. Standardna ping naredba obično koristi 56 bajta podataka, pa s IP i ICMP zaglavljem ukupna veličina može biti 64 bajta.
**m) Postavi filter da se prati samo ICMP protokol.**
U Wiresharku možemo koristiti filter icmp
**n) Koliko je ICMP echo i reply paketa?**
Nakon filtriranja ICMP prometa, broj ICMP echo request i echo reply paketa trebao bi biti jednak, jer za svaki echo request postoji echo reply. Broj tih paketa ovisi o broju poslanih ping zahtjeva.
**o) Koji protokol pokreće naredba ping?**
Naredba ping koristi ICMP protokol.
**p) Sastavni dio kojeg protokola je protokol ICMP?**
ICMP je dio IP protokola.
**q) U koji okvir je enkapsuliran IP paket?**
IP paket je enkapsuliran u Ethernet okvir (ako koristiš Ethernet mrežu).