

LV2: Osnovna analiza mrežnog prometa

Karlo Flegar 3.a, 29.9.2023.

PRIPREMA ZA VJEŽBU:

1. Što je i čemu služi protokol ARP?
Protokol ARP je Address Resolution Protocol, tj. komunikacijski je protokol za određivanje fizičkih adresa, a služi za dobivanje fizičke adrese (MAC adrese) iz poznate logičke (IPv4) adrese.
2. Što je i čemu služi protokol ICMP?
ICMP je komunikacijski protokol koji je ugrađen u svaki IP modul kako bi usmjernicima ili računalima omogućio slanje kontrolnih poruka o greškama, a služi prijavljivanju grešaka bez njihovog ispravljanja.
3. Što znaš o naredbi ping?
Naredba ping je osnovni mrežni alat koji služi za provjeru dostupnosti određenog hosta povezanog u IP mrežu. U naredbenom retku se zadaje ili ping hostname za provjeru povezanosti s nekom stranicom, ili ping IPv4 adresa kako bi smo provjerili povezanost s računalom.

IZVOĐENJA VJEŽBE:

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

```
C:\WINDOWS\system32>netsh interface ipv4 show config

Configuration for interface "Ethernet"
  DHCP enabled:                No
  IP Address:                  192.168.10.3
  Subnet Prefix:              192.168.10.0/24 (mask 255.255.255.0)
)
  Default Gateway:            192.168.10.1
  Gateway Metric:              256
  InterfaceMetric:            25
  Statically Configured DNS Servers:  None
  Register with which suffix:  Primary only
  Statically Configured WINS Servers:  None

Configuration for interface "Npcap Loopback Adapter"
  DHCP enabled:                Yes
  IP Address:                  169.254.222.39
  Subnet Prefix:              169.254.0.0/16 (mask 255.255.0.0)
  InterfaceMetric:            25
  DNS servers configured through DHCP:  None
  Register with which suffix:  Primary only
  WINS servers configured through DHCP:  None

Configuration for interface "Loopback Pseudo-Interface 1"
  DHCP enabled:                No
  IP Address:                  127.0.0.1
  Subnet Prefix:              127.0.0.0/8 (mask 255.0.0.0)
  InterfaceMetric:            75
  Statically Configured DNS Servers:  None
  Register with which suffix:  None
  Statically Configured WINS Servers:  None

C:\WINDOWS\system32>netsh interface ipv4 set address name="Ethernet" static 1
192.168.10.3 255.255.255.0 192.168.10.1

C:\WINDOWS\system32>ipconfig /all

Windows IP Configuration

Host Name . . . . . : WS3_LAB_2_3
Primary Dns Suffix . . . . . :
Node Type . . . . . : Hybrid
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No

Ethernet adapter Ethernet:

Connection-specific DNS Suffix . :
Description . . . . . : Realtek PCIe GBE Family Controller
Physical Address. . . . . : 70-85-C2-CE-9B-92
DHCP Enabled. . . . . : No
Autoconfiguration Enabled . . . . : Yes
Link-local IPv6 Address . . . . . : fe80::1deb:f0c0:47f6:aaf8%5(Preferred)

IPv4 Address. . . . . : 192.168.10.3(Preferred)
Subnet Mask . . . . . : 255.255.255.0
```

```

C:\WINDOWS\system32>ipconfig /all

Windows IP Configuration

Host Name . . . . . : WS3_LAB_2_3
Primary Dns Suffix . . . . . :
Node Type . . . . . : Hybrid
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No

Ethernet adapter Ethernet:

Connection-specific DNS Suffix . :
Description . . . . . : Realtek PCIe GBE Family Controller
Physical Address. . . . . : 70-85-C2-CE-9B-92
DHCP Enabled. . . . . : No
Autoconfiguration Enabled . . . . : Yes
Link-local IPv6 Address . . . . . : fe80::1deb:f0c0:47f6:aaf8%5(Preferred)

IPv4 Address. . . . . : 192.168.10.3(Preferred)
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.10.1
DHCPv6 IAID . . . . . : 40928706
DHCPv6 Client DUID. . . . . : 00-01-00-01-25-1F-D5-CA-70-85-C2-CE-9B
-92
DNS Servers . . . . . : fec0:0:0:ffff::1%1
                        fec0:0:0:ffff::2%1
                        fec0:0:0:ffff::3%1
NetBIOS over Tcpi. . . . . : Enabled

Ethernet adapter Npcap Loopback Adapter:

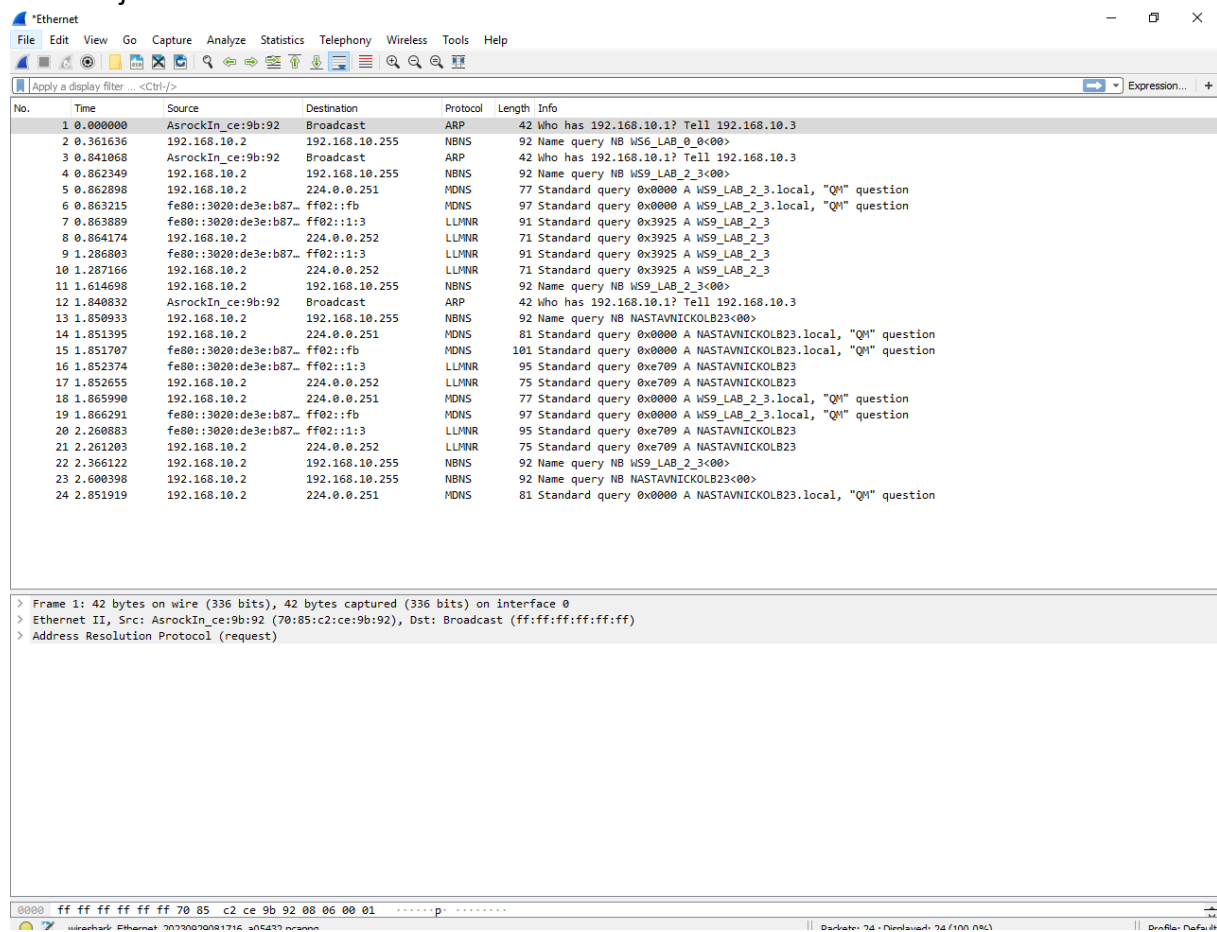
Connection-specific DNS Suffix . :
Description . . . . . : Npcap Loopback Adapter
Physical Address. . . . . : 02-00-4C-4F-4F-50
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
Link-local IPv6 Address . . . . . : fe80::710f:6bbc:5967:de27%10(Preferred
)
Autoconfiguration IPv4 Address. . : 169.254.222.39(Preferred)
Subnet Mask . . . . . : 255.255.0.0
Default Gateway . . . . . :
DHCPv6 IAID . . . . . : 201457740
DHCPv6 Client DUID. . . . . : 00-01-00-01-25-1F-D5-CA-70-85-C2-CE-9B
-92
DNS Servers . . . . . : fec0:0:0:ffff::1%1
                        fec0:0:0:ffff::2%1
                        fec0:0:0:ffff::3%1
NetBIOS over Tcpi. . . . . : Enabled

C:\WINDOWS\system32>

```

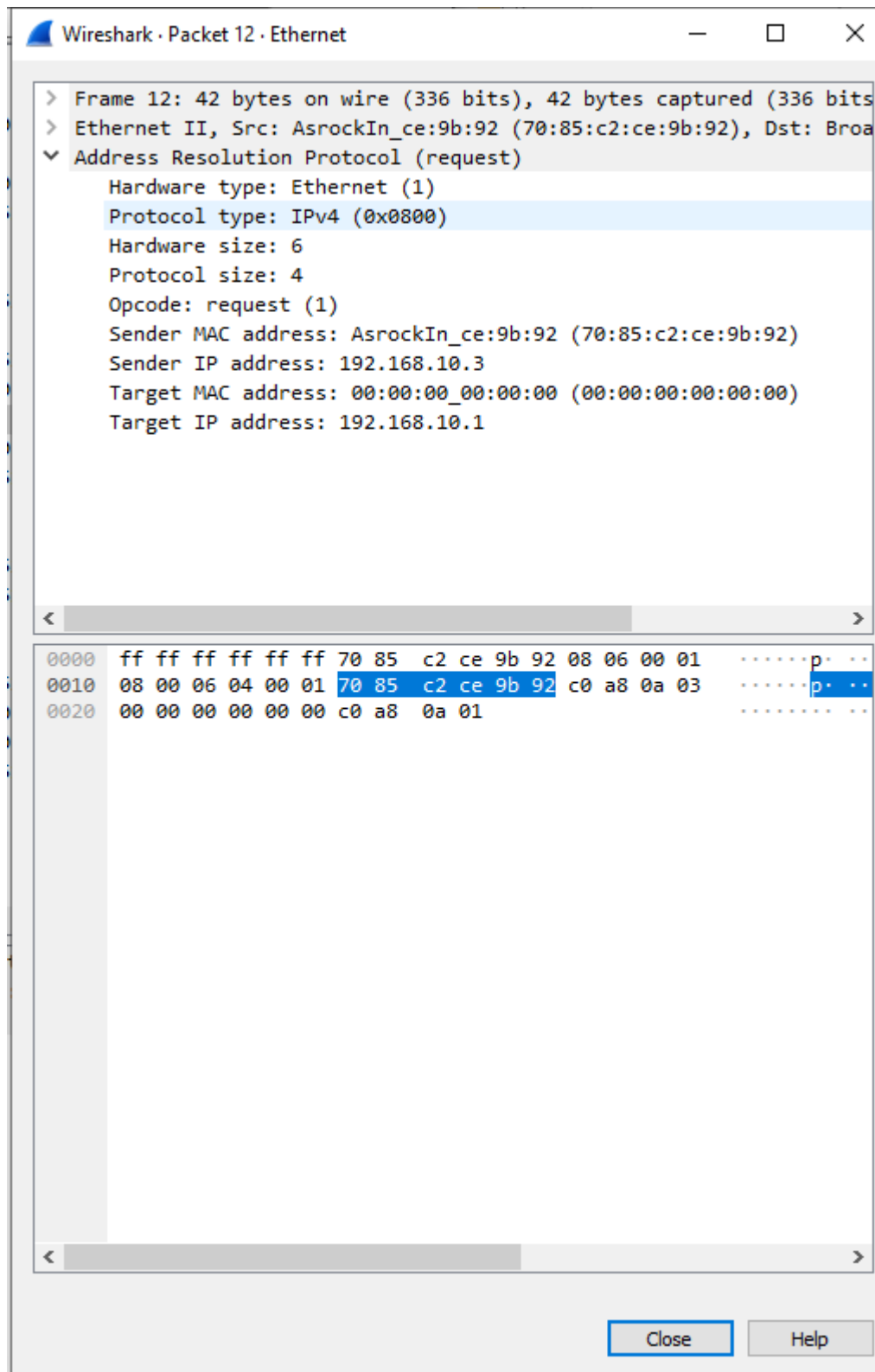
3. Pokrenuti program Wireshark. Pričekati da se prikaže prvih dvadesetak redaka, a onda zaustaviti hvatanje (Capture – Stop).

- a. Koliko je točno okvira Wireshark „uhvatio“?
Uhvatio je 24 okvira.



- b. Koje su oznake protokola na tim okvirima?
NBNS, MDNS, LLMNR, ARP.
- c. Koristeći dostupne informacije sa predavanja/Interneta opiši kratko funkcije tih protokola.
NBNS -
MDNS-
LLMNR – Link_Local Multicast Name Resolution je protokol temeljen na formatu paketa DNS (Domain Name System) koji omogućuje IPv4 i IPv6 hostovima da izvrše razrješenje imena za hostove u lokalnoj vezi.
- d. Analiziraj okvir koji u sebi nosi:
➤ ARP paket (protokol) request te ispiši:
1. Polazišnu MAC adresu
70:85:c2:ce:9b:92
2. Odredišnu MAC adresu
00:00:00:00:00:00
3. Polazišnu IP adresu
192.168.10.3

4. Odredišnu IP adresu
192.168.10.1



- ARP paket (protokol) – reply
1. Polazišnu MAC adresu
 2. Odredišnu MAC adresu
 3. Kolika je veličia svake od ovih adresa?
 4. Polazišnu IP adresu

5. Odredišnu IP adresu

- e. Kako glasi odredišna MAC adresa prvog Ethernet okvira kod ARP protokola i zašto?
4. Zadatak
5. Računala ponovno spojiti u školsku mrežu i provjeriti mrežne postavke. Učitati tri web stranice po želji i pratiti promet na vezi pomoću alata Wireshark.