LV 2: Osnovna analiza mrežnog prometa
Šiletić_Škrabec_3.C

PRIPREMA ZA VJEŽBU

U pisanoj formi odgovori na slijedeća pitanja:

1. Što je i čemu služi protokol ARP?

ARP (eng. Address Resolution Protocol) – komunikacijski protokol kojim se dobiva fizička adresa na lokalnoj mreži iz poznate mrežne adrese. Najraširenija njegova primjena danas je na Ethernetu gdje se IP adrese povezuju s MAC adresama.

2. Što je i čemu služi protokol ICMP?

ICMP (eng. Internet Control Message Protocol) – komunikacijski protokol koji je ugrađen u svaki IP modul da bi omogućio mrežnim prolazima (usmjerivačima) ili računalima slanje kontrolnih poruka o greškama. Zadužen je samo za prijavljivanje grešaka, ali ne i za njihovo ispravljanje.

3. Što znaš o naredbi ping?

Naredba ping omogućava ispitivanje povezanosti između računala na kojem se naredba koristi i bilo kojeg od ostalih računala i čvorova u mreži. Ova naredba šalje upit prema navedenom odredišnom računalu te na taj upit odredišno računalo odgovara.

IZVOĐENJE VJEŽBE

1. zadatak

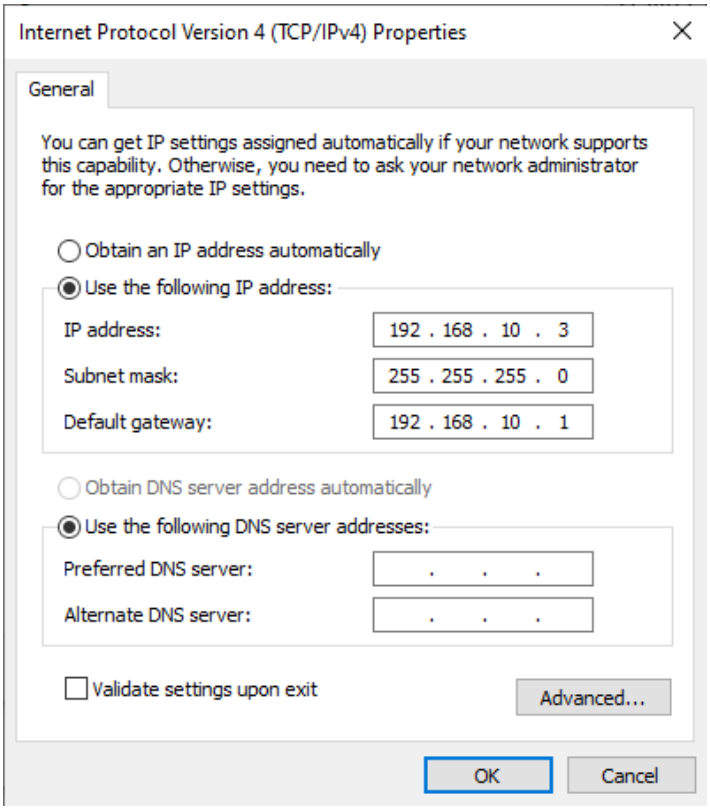
Povezati dva susjedna računala odgovarajućim kabelom te uspostaviti P2P spoj.

Povezali smo računala.

2. zadatak

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. zadatak

Pokrenuti program Wireshark.

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

No.	Time	Source	Destination	Protocol	Lengtl	Info
1	0.000000	MicroStarINT_c7:53:…	Broadcast	ARP	42	Who has 192.168.10.1? Tell 192.168.10.3
2	0.841237	MicroStarINT_c7:53:…	Broadcast	ARP	42	Who has 192.168.10.1? Tell 192.168.10.3
3	1.834586	MicroStarINT_c7:53:…	Broadcast	ARP	42	Who has 192.168.10.1? Tell 192.168.10.3
4	2.200866	192.168.10.3	192.168.10.2	ICMP	74	Echo (ping) request id=0x0001, seq=1/256, ttl=128 (repl
5	2.201381	192.168.10.2	192.168.10.3	ICMP	74	Echo (ping) reply id=0x0001, seq=1/256, ttl=128 (requ
6	3.211856	192.168.10.3	192.168.10.2	ICMP	74	Echo (ping) request id=0x0001, seq=2/512, ttl=128 (repl
7	3.212299	192.168.10.2	192.168.10.3	ICMP	74	Echo (ping) reply id=0x0001, seq=2/512, ttl=128 (requ
8	4.227827	192.168.10.3	192.168.10.2	ICMP	74	Echo (ping) request id=0x0001, seq=3/768, ttl=128 (repl
9	4.228296	192.168.10.2	192.168.10.3	ICMP	74	Echo (ping) reply id=0x0001, seq=3/768, ttl=128 (requ
10	4.865442	MicroStarINT_c7:52:…	Broadcast	ARP	60	Who has 192.168.10.1? Tell 192.168.10.2
11	5.240515	192.168.10.3	192.168.10.2	ICMP	74	Echo (ping) request id=0x0001, seq=4/1024, ttl=128 (rep
12	5.241032	192.168.10.2	192.168.10.3	ICMP	74	Echo (ping) reply id=0x0001, seq=4/1024, ttl=128 (req
13	5.422411	MicroStarINT_c7:52:…	Broadcast	ARP	60	Who has 192.168.10.1? Tell 192.168.10.2
14	6.435176	MicroStarINT_c7:52:…	Broadcast	ARP	60	Who has 192.168.10.1? Tell 192.168.10.2
15	6.830655	MicroStarINT_c7:53:…	MicroStarINT_c7:52:…	ARP	42	Who has 192.168.10.2? Tell 192.168.10.3
16	6.831138	MicroStarINT_c7:52:…	MicroStarINT_c7:53:…	ARP	60	192.168.10.2 is at 04:7c:16:c7:52:c0
17	6.894614	MicroStarINT_c7:53:…	Broadcast	ARP	42	Who has 192.168.10.1? Tell 192.168.10.3
18	6.922787	MicroStarINT_c7:52:…	MicroStarINT_c7:53:…	ARP	60	Who has 192.168.10.3? Tell 192.168.10.2
19	6.922824	MicroStarINT_c7:53:…	MicroStarINT_c7:52:…	ARP	42	192.168.10.3 is at 04:7c:16:c7:53:29
20	7.837505	MicroStarINT_c7:53:…	Broadcast	ARP	42	Who has 192.168.10.1? Tell 192.168.10.3
21	8.830615	MicroStarINT_c7:53:…	Broadcast	ARP	42	Who has 192.168.10.1? Tell 192.168.10.3
22	8.993169	MicroStarINT_c7:52:…	Broadcast	ARP	60	Who has 192.168.10.1? Tell 192.168.10.2

a) Koliko je točno okvira Wireshark „uhvatio“?

Uhvatio je 22 okvira.

b) Koje su oznake protokola na tim okvirima?

ARP, ICMP

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

ARP - komunikacijski protokol kojim se dobiva fizička adresa na lokalnoj mreži iz poznate mrežne adrese.

ICMP - komunikacijski protokol koji je ugrađen u svaki IP modul da bi omogućio mrežnim prolazima (usmjerivačima) ili računalima slanje kontrolnih poruka o greškama.

d) Analiziraj okvir koji u sebi nosi:

ARP paket (protokol) request te ispiši:

- polazišnu MAC adresu

04:7c:16:c7:53:29

- odredišnu MAC adresu

04:7c:16:c7:52:c0

- polazišnu IP adresu

192.168.10.3

- odredišnu IP adresu

192.168.10.2

ARP paket (protokol) – reply te ispiši:

- polazišnu MAC adresu

04:7c:16:c7:52:c0

- odredišnu MAC adresu

04:7c:16:c7:53:29

- Kolika je veličina svake od ovih adresa?

48 bita

- 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?

Glasi ff:ff:ff:ff:ff:ff zato što je to broadcast MAC adresa.

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?

4 ICMP echo i reply paketa.

b) Koji protokol pokreće naredba ping?

Pokreće protokol ICMP.

c) Sastavni dio kojeg protokola je ICMP protokol?

Sastavni je dio IP-a.

d) U koji okvir je enkapsuliran IP paket?

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

pitanja:

e) Koja je polazišna IP adresa?

192.168.10.3

f) Koja je odredišna IP adresa?

192.168.10.2

g) Koja je MAC adresa polazišnog uređaja?

04:7c:16:c7:53:29

h) Koja je MAC adresa odredišnog uređaja?

04:7c:16:c7:52:c0

i) Koja je oznaka vrste podataka u Ethernet okviru?

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

Velicina IP adrese je 32 bita, a MAC adrese je 48 bita.

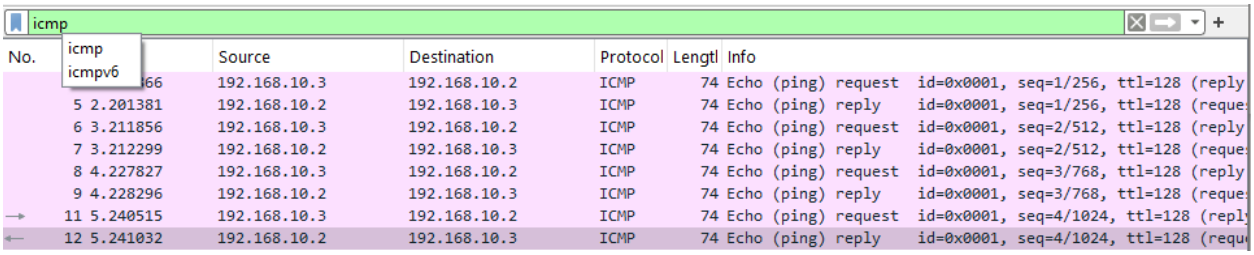
k) Koja je veličina IP paketa kod ICMP protokola?

74 bajta.

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

32 bajta.

m) Postavi filter da se prati samo ICMP protokol.



5. Zadatak

Računala ponovno spojiti u školsku mrežu i provjeriti mrežne postavke.

Učitati tri web stranice po želji i pratiti promet na vezi pomoću alata Wireshark.