LV02: Osnovna analiza mrežnog prometa

Priprema za vježbu:

1) Što je i čemu služi protokol ARP?

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

2) Što je i čemu služi protokol ICMP?

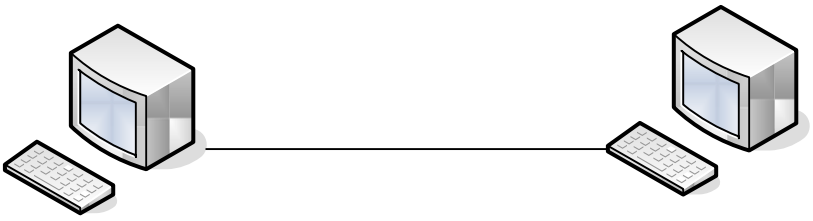
ICMP je komunikacijski protokol ugrađen u svaki IP modul kako bi usmjernicima/računalima omogućio slanje kontrolnih poruka o greškama

3) Što znaš o naredbi ping?

Ping je naredba koja se koristi kao osnovni mrežni alat koji služi za provjeru dostupnosti određenog hosta povezanog u IP mrežu

Izvođenje vježbe:

1) Povezati dva susjedna računala odgovarajućim kabelom te uspostaviti P2P spoj.



PC1 PC2

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).

a) Koliko je točno okvira Wireshark „uhvatio“?

32

b) Koje su oznake protokola na tim okvirima?

DHCP, SSDP, BROWSER

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

SSDP (Simple Service Discovery Protocol) mrežni je protokol temeljen na paketu internetskih protokola za oglašavanje i otkrivanje mrežnih usluga i informacija o prisutnosti.

DHCP (Dynamic Host Configuration Protocol) mrežni je protokol korišten od strane mrežnih računala za dodjeljivanje IP adresa i ostalih mrežnih postavki

d) Analiziraj okvir koji u sebi nosi:

ARP paket (protokol) request te ispiši:

polazišnu MAC adresu

odredišnu MAC adresu

polazišnu IP adresu

odredišnu IP adresu

ARP paket (protokol) – reply te ispiši:

polazišnu MAC adresu

kolika je veličina svake od ovih adresa?

odredišnu MAC adresu

polazišnu IP adresu

odredišnu IP adresu

ARP Request

```
> Frame 1: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface 0
> Ethernet II, Src: AsrockIn_ce:9a:f7 (70:85:c2:ce:9a:f7), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
v Address Resolution Protocol (request)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: request (1)
    Sender MAC address: AsrockIn_ce:9a:f7 (70:85:c2:ce:9a:f7)
    Sender IP address: 192.168.10.2
    Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)
    Target IP address: 192.160.10.1
```

ARP Reply

```
> Frame 15: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface 0
> Ethernet II, Src: AsrockIn_ce:9a:f7 (70:85:c2:ce:9a:f7), Dst: AsrockIn_ce:9a:f0 (70:85:c2:ce:9a:f0)
v Address Resolution Protocol (reply)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: reply (2)
    Sender MAC address: AsrockIn_ce:9a:f7 (70:85:c2:ce:9a:f7)
    Sender IP address: 192.168.10.2
    Target MAC address: AsrockIn_ce:9a:f0 (70:85:c2:ce:9a:f0)
    Target IP address: 192.168.10.3
```

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

```
> Frame 1: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface 0
> Ethernet II, Src: AsrockIn_ce:9a:f7 (70:85:c2:ce:9a:f7), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
v Address Resolution Protocol (request)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: request (1)
    Sender MAC address: AsrockIn_ce:9a:f7 (70:85:c2:ce:9a:f7)
    Sender IP address: 192.168.10.2
    Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)
    Target IP address: 192.160.10.1
```

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

b) Koji protokol pokreće naredba ping?
ICMP protokol
c) Sastavni dio kojeg protokola je ICMP protokol?
IPv4 protokol
d) U koji okvir je enkapsuliran IP paket?

Ethernet 1 okvir

Izaberi jedan redak koji se odnosi na protokol ICMP, ispiši njegov sadržaj te odgovori na slijedeća pitanja:
a) Koja je polazišna IP adresa?
192.168.10.2
b) Koja je odredišna IP adresa?
192. 168.10.3

c) Koja je MAC adresa polazišnog uređaja?

(70:85:c2:ce:9a:f7)

d) Koja je MAC adresa odredišnog uređaja?

(70:85:c2:ce:9a:f0)

e) Koja je oznaka vrste podataka u Ethernet okviru?

Type: IPv4 (0x0800)

f) Koja je veličina IP adrese, a koja MAC adrese u okvirima/paketima?
Veličina IP adrese je 4B,a MAC adrese 6B
g) Koja je veličina IP paketa kod ICMP protokola?

Veličina IP paketa kod ICMP protokola je : 60

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

Veličina paketa (Total length) – Veličina zaglavlja (Header length)= 60-20=40, veličina podataka je 40

i) Postavi filter da se prati samo ICMP protokol.
Postavimo filter u Wiresharku, u pretraživač upišemo ICMP
j) Koliko je ICMP echo i reply paketa?
8 sveukupno, 4 echo paketa i 4 reply paketa
k) Koji protokol pokreće naredba ping?
Pokreće protokol ICMP

l) Sastavni dio kojeg protokola je protokol ICMP?

Sastavni je dio IP protokola
m) U koji okvir je enkapsuliran IP paket?
Enkapsuliran je u okvir Ethernet 1

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.

Nakon obavljenih zadataka u ovoj vježbi učenik će znati samostalno (ili uz manju pomoć zabilješki): Pratiti i analizirati promet na vezi sa programom za praćenje protokola

Nakon ponovnog spajanja u mrežu provjerili smo mrežne postavke i nastavili pratiti promet na vezi pomoću Wiresharka