LV02: Osnovna analiza mrežnog prometa

Priprema

1. Što je i čemu služi protokol ARP?
ARP (Addres Resolution Protocol) se koristi za dobivanje fizicke adrese od poznate mrezne adrese.

2. Što je i čemu služi protokol ICMP?
ICMP (Internet Control Message Protocol) je protokol kojim se salju kontrolne poruke ili poruke o greskama.

3. Što znaš o naredbi ping?
Naredbom ping se provjerava medusobna spojenost izmedu racunala u mrezi. Vrlo korisna dijagnosticka naredba. Koristi ICMP echo.

Izvodenje

3.

a) Koliko je točno okvira Wireshark „uhvatio“?
146
b) Koje su oznake protokola na tim okvirima?
ARP, SSDP, ICMP, BROWSER
c) Koristeći dostupne informacije sa predavanja/Interneta opiši kratko funkcije tih protokola.
ARP dobavlja fizicku adresu od poznate mrezne adrese, SSMP advertizira servise u malim mrezama, ICMP se koristi za kontrolne poruke i poruke o greskama, BROWSER je windowsov browser protocol.
d) Analiziraj okvir koji u sebi nosi:
    a. ARP paket request
    polazisni MAC: 70:85:c2:ce:9b:90
    odredisni MAC: 00:00:00:00:00:00
    polazisni IP: 192.168.10.2
    odredisni IP: 192.168.10.1
    b. ARP paket reply
    polazisni MAC: 70:85:c2:ce:9b:90
    odredisni MAC: 70:85:c2:ce:9b:a8
    velicina adresa: 6 bajtova
    polazisni IP: 192.168.10.2
    odredisni IP: 192.168.10.3
e) Kako glasi odredišna MAC adresa prvog Ethernet okvira kod ARP protokola i zašto?
ff:ff:ff:ff:ff:ff jer je to broadcast MAC adresa.

4. U istom spoju računala pomoću Wiresharka analiziraj ICMP promet korištenjem naredbe ping sa jednog računala na drugo.

a) Ima 4 ICMP echo i reply paketa
b) Pokrece ICMP protokol
c) ICMP je sastavni dio IPv4 protokola
d) IP okvir je enkapsuliran u zaglavlju paketa

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
f) Koja je odredišna IP adresa?	192.168.10.3
g) Koja je MAC adresa polazišnog uređaja?	70:85:c2:ce:9b:a8
h) Koja je MAC adresa odredišnog uređaja?	70:85:c2:ce:9b:90
i) Koja je oznaka vrste podataka u Ethernet okviru?	IPv4
j) Koja je veličina IP adrese, a koja MAC adrese u okvirima/paketima?	IP 4 byta, MAC 6
k) Koja je veličina IP paketa kod ICMP protokola?	20 byta
l) Koja je veličina podataka u IP paketu kod ICMP protokola?	20 byta
m) Postavi filter da se prati samo ICMP protokol.	60
n) Koliko je ICMP echo i reply paketa?	16
o) Koji protokol pokreće naredba ping?	Pokrece ICMP
p) Sastavni dio kojeg protokola je protokol ICMP?	Dio IPv4 protokola
q) U koji okvir je enkapsuliran IP paket?	Enkapsuliran je u zaglavlju paketa

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.

Normalan rad i funkcija paketa prilikom ucitavanja stranica.