1. Katera polja okvira Ethernet II vam prikaže Wireshark? Razmislite o razlogih, zakaj ne prikaže vsa polja?

-source mac, destination mac, type, data.... CRC ne vidimo -ker ni napak... ga ni zajelo

-zacne se šele po sfdju

2. Kakšna je celotna dolžina okvira Ethernet II v prvem paketu? Kaj pa dolžina podatkov?

- 74B, 60B podatkov.. 14 pa glava

3. Kakšen je prejemnikov naslov v prvem okvirju? Katero podjetje je izdelovalec prejemnikove mrežne kartice?

- 00:12:43:3b:23:ff - Cisco Systems, Inc

4. V zadnjem casu so zaceli spet razvijati Ethernet nižjih hitrosti, to je 2,5 in 5 Gbit/s Ethernet.

Kaj misliš, zakaj? Ali lahko najdeš kakšen prakticen primer uporabe, kjer so ravno te hitrosti najbolj primerne?

- prehitro za hardware, da lahko preko starih žic transferamo

2. naloga:

HUB RAZDELI VSE OKVIRJE NA OSTALE---tako da ta ko je samo prejemov je dubu use pakete k so jih ostali sharal med sabo

Najprej smo uporabili razdelilnik (hub) in na racunalnikih B in C zajeli promet s programom Wireshark. S programom Wireshark odprite spodnji datkoteki:

ping\_hub\_B.cap: promet zajet na racunalniku B pri uporabi razdelilnika.

ping\_hub\_C.cap: promet zajet na racunalniku C pri uporabi razdelilnika.

Napišite filter, ki vam bo prikazal samo pakete ping (protokol ICMP) in odgovorite na spodnja vprašanja:

1. Koliko racunalnikov je udeleženih v komunikaciji? Namig: Statistics, Conversations, vklopite tudi opcijo Limit to display filter.

-3je linksysG, 3com ,dellComp

2. Kakšna strojna naslova imata prejemnika ICMP echo request sporocil?

-request -192.168.0.104- pač njegov mac.. neda se mi pisat

3. Koliko paketov ICMP je v datoteki ping\_hub\_B.cap? Koliko paketov ICMP je v datoteki ping\_hub\_C.cap? So paketi v obeh datotekah enaki ali se razlikujejo?

-28 paketov v B in C

4. Razloži, ali smo na racunalniku C uporabili promiscuous mode zajemanja?

-da, ker smo dobili nefiltrirano (ali pač)?

S programom Wireshark odprite še datoteki:

ping\_switch\_B.cap: promet zajet na racunalniku B pri uporabi stikala.

ping\_switch\_C.cap: promet zajet na racunalniku C pri uporabi stikala.

Odgovorite še na spodnja vprašanja:

Koliko racunalnikov je vkljucenih v komunikacijo v datoteki ping\_switch\_B.cap?

-3je isti promet je... ker je B itaq dobivala ves promet

Koliko racunalnikov je vkljucenih v komunikacijo v datoteki ping\_switch\_C.cap?

2 -racunalnik A in HDCP

Katerih paketov ne vidimo v datoteki ping\_switch\_B.cap, so pa v datoteki ping\_hub\_B.cap? Zakaj?

ne vidimo broadcast pinge... ker stikalo pošle sam na port kjer je treba

WIFI:

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*//PONOVIIIIII!!!!\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

NALOGA3:

1.Oglejte si okvir Beacon (Beacon frame). Katera polja se nahajajo v okvirju 802.11? Na kratko opišite njihov pomen.

4 mac adressi, uporabljajo se 3je(kdo,komu,cez katero bazno postajo), dela preko CSMA/cs... beacon frame- pogleda prisotnost.. 10x na sekundo pošlje beaconframe

2.Kakšen je BSS ID omrežja? Kaj pa SSID (poglejte tudi parametre v 802.11 Wireless LAN Management frame)?

SSID-logicno ime omrežja...(name),

BSSID- mac access point

3.Kako je nastavljen bit Privacy, ki je del Capability Information?

0->to je potem openWifi

protected flag - (data is not protected)-niso kriptirani.. beacon podatki ne smejo biti kriptirani

0->nekriptirana

4.V programu Wireshark napišite filter, ki vam bo prikazal samo okvirje, ki vsebujejo podatke (data frames). Kateri filter ste uporabili?

wlan\_mgt ->podatkovni frami !!!!!!!!!!!!!!!!!!!!!

5.Kako je nastavljena zastavica Protected, ki je del kontrolnih bitov okvira 802.11?

?

V nekoliko drugacnem brezžicnem omrežju (torej ne takšnem, kot je na zgornji sliki) smo omogocili

šifriranje WPA, s programom Wireshark pa smo zajeli promet, ki ga je eden od racunalnikov pošiljal v Internet.

Odprite datoteko wpa.cap in odgovorite še na spodnja vprašanja:

1. Kako je nastavljena zastavica Protected v okvirjih Beacon v datoteki wpa.cap?

2. Kako je nastavljen bit Privacy, ki je del Capability Information?

3. Uporabite filter, ki vam bo prikazal samo podatkovne okvire in poglejte zastavico Protected v polju Frame Control. Kako se razlikuje v primerjavi z datoteko nowep.cap?

->wlan\_mgt

4. V programu Wireshark lahko tudi dekriptirate omrežni promet, ce seveda veste uporabljeno geslo. Datoteko wpa.cap najprej natancno poglejte brez dešifriranja (pomembni so podatkovni okvirji - data frames - nastavite si ustrezen filter). Nato izberite v meniju Edit, Preferences. Med protokoli poišcite IEEE 802.11, obkljukajte Enable Decryption, v polje Decryption Keys pa vnesite: wpa-pwd in vrednost Induction. Kaj opazite sedaj? (namig: najvec se dogaja tam nekje od 430. paketa naprej).

[Težje, neobvezno vprašanje (ker še nismo obravnavali HTTP protokola): Ali lahko poišceš spletno stran, ki jo je obiskal uporabnik, katerega promet smo zajeli v tej datoteki?]

Po vaji si dekripcijski filter izkljucite (Edit, Preferences, med protokoli poišcite IEEE 802.11, Enable Decryption naj ne bo oznacen!)

\*\*\*\*\*\*\*\*\*\*\*ARP\*\*\*TODO.. DID NOTHING DONT UNDERSTAND NOTHING\*\*\*\*\*\*\*\*\*\*\*

VAJA4: ARP

S programom Wireshark odprite datoteko arp.cap in odgovorite na spodnja vprašanja:

1.Kakšen je strojni naslov prejemnika zahteve ARP (ARP request)?

00:50:56:88:13:bd

2.Kakšen je strojni naslov pošiljatelja odgovora ARP (ARP reply)?

ff:ff:ff:ff:ff:ff

3.Kakšna je vsebina polj pri protokolu ARP v prvem paketu?

4.Oglejte si zahtevo ARP. Ali je v njej kakšen neznan naslov? Zakaj?

5.Lahko morda najdete kakšen neznan naslov pri odgovoru ARP? Zakaj?

Odprite ukazno vrstico na vašem racunalniku in odgovorite na spodnja vprašanja:

Kateri ukaz morate na vašem operacijskem sistemu uporabiti za izpis tabele ARP?

Kako bi na operacijskem sistemu, ki ga trenutno uporabljate, v tabelo ARP dodali vnos za racunalnik z IP-jem 192.168.254.10 in strojnim naslovom 12:34:56:aa:bb:aa?

Kako bi na operacijskem sistemu, ki ga trenutno uporabljate, pobrisali vsebino tabele ARP?

Vprašajte kolega, ki sedi na sosednjem racunalniku po njegovem naslovu IP in MAC. Ta racunalnik mora biti v istem segmentu, kot je vaš racunalnik. (Zakaj?) Poglejte, ali je ta vnos IP in MAC v vaši ARP tabeli.

Sosedu pošljite ping in nato ponovno poglejte svojo ARP tabelo. Pokukajte še k sosedu in si oglejte njegovo ARP tabelo...