Lab 3.1: Wireshark labor: Ethernet ja ARP v8.0

Video: https://www.youtube.com/watch?v=sWCDj7sS7hs

Eng: https://www-net.cs.umass.edu/wireshark-labs/Wireshark_Ethernet_ARP_v8.0.pdf

Täienduseks raamatule: Computer Networking: A Top-Down Approach, 8. väljaanne, J.F. Kurose ja K.W. Ross

"Ütle mulle ja ma unustan. Näita mulle ja ma mäletan. Kaasa mind ja ma saan aru."
— Hiina vanasõna

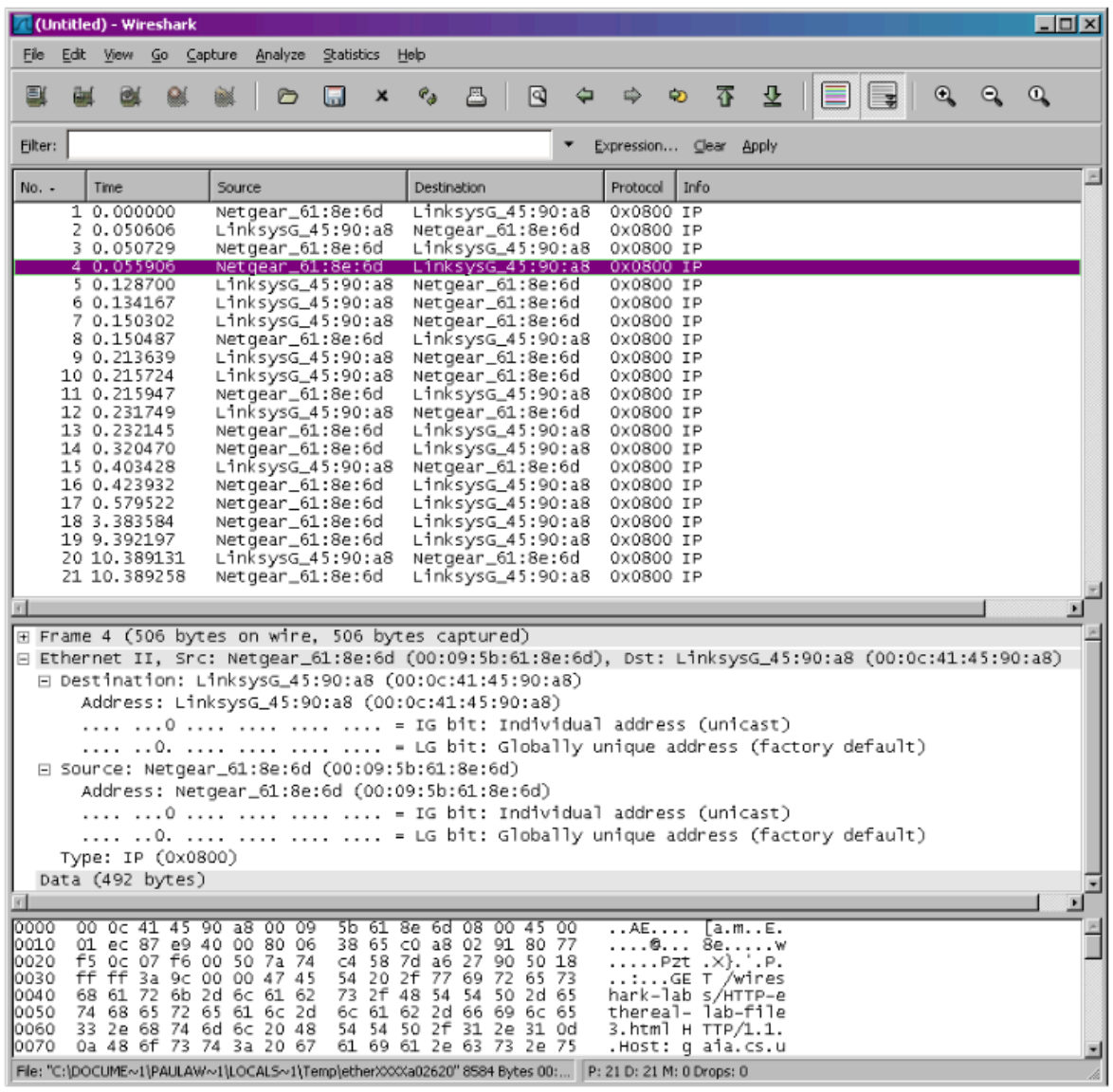
Sissejuhatus:

Selles laboris uurime **Etherneti** ja **ARP** protokolle. Enne selle labori alustamist tasub üle vaadata peatükid **6.4.1 (Linki-kihi aadresseerimine ja ARP)** ja **6.4.2 (Ethernet)** tekstist. **RFC 826** (ftp://ftp.rfc-editor.org/in-notes/std/std37.txt) sisaldab ARP protokolli üksikasjalikku kirjeldust, mida kasutatakse, et IP-seade määraks kaugarvuti liidese IP-aadressi, mille Etherneti aadress on teada.

1. Etherneti raamide püüdmine ja analüüsimine

Alustame Etherneti raamide kogumise ja uurimisega. Tee järgmist:

1. **Tühjenda oma brauseri vahemälu**:
   Firefoxis vali **Tools->Clear Recent History** ja märgi kasti "Cache". Internet Exploreris vali **Tools->Internet Options->Delete Files**.
2. **Käivita Wireshark**:
   Ava Wiresharki pakettide püüdmise tööriist.
3. **Mine järgmisele veebilehele**:
   http://gaia.cs.umass.edu/wireshark-labs/HTTP-ethereal-lab-file3.html
   Sinu brauser peaks kuvama USA põhiseaduse õiguste loetelu.
4. **Lõpeta Wiresharki paketipüüdmine**:
   Leia paketid, mis sisaldavad **HTTP GET** sõnumit, mis saadeti sinu arvutist aadressile **gaia.cs.umass.edu**, ning ka **HTTP vastuse** sõnumid, mis tulid sinu arvutisse.
   Kuna see labor keskendub Ethernetile ja ARP-le, ei huvita meid kõrgema taseme protokollid, nagu IP. Muuda Wiresharki seadistust nii, et see kuvaks ainult protokolle, mis on alla IP-taseme. Tee seda, valides **Analyze->Enabled Protocols** ja eemaldades märgistus **IP** kastist. Nüüd peaksid nägema ainult Etherneti ja ARP protokolle.



Järgmistele küsimustele vastamiseks pead vaatama Wiresharki paketi detailide ja sisu aknasse (Wiresharki keskmine ja alumine aken):

Vali Etherneti raam, mis sisaldab **HTTP GET** sõnumit. (Meenuta, et **HTTP GET** sõnum on pakitud **TCP segmendi** sisse, mis omakorda on pakitud **IP datagrammi**, mis lõpuks on pakitud **Etherneti raamisse**. Kui see kapseldamine tundub segadusttekitav, loe uuesti peatükki **1.5.2** tekstist.) Laienda **Ethernet II** infot paketi detailide aknas. Pane tähele, et Etherneti raami sisu (nii päis kui ka andmed) kuvatakse paketi sisu aknas.

Vasta järgmistele küsimustele, mis põhinevad **HTTP GET** sõnumit sisaldava Etherneti raami sisul. Kui võimalik, siis prindi välja jälgitavad paketid, mida kasutasid vastuste andmiseks. **Lisa väljatrükile selgitusi**, et selgitada oma vastuseid. Paketi printimiseks mine **File -> Print**, vali **Selected packet only** (ainult valitud pakett), vali **Packet summary line** (paketi kokkuvõtte rida) ja vali vastav detailide hulk, mida vajad vastamiseks.

Küsimused (Ethernet-raamide analüüsimiseks):

1: Mis on sinu arvuti 48-bitine Etherneti aadress?

- **Vihje:** Sinu arvuti Etherneti aadress on tuntud ka kui MAC-aadress. Selle leiad, kui valid Etherneti raami, milles on **HTTP GET** sõnum.
- **Kuidas otsida:** Laienda Wiresharki aknas **Ethernet II** sektsioon ja vaata välja **Source MAC Address**. See on sinu arvuti 48-bitine MAC-aadress.

2: Mis on sihtaadress Etherneti raamis? Kas see on aadress gaia.cs.umass.edu? Kui ei, siis millise seadme Etherneti aadress see on?

- **Vihje:** Sihtaadress on MAC-aadress, millele saadetakse pakett. Veendu, et sa eristad IP-aadresse ja MAC-aadresse, sest need on erinevad.
- **Kuidas otsida:** Laienda **Ethernet II** sektsioon Wiresharkis ja vaata välja **Destination MAC Address**. Sihtaadress ei ole tavaliselt veebilehe, nagu gaia.cs.umass.edu, aadress, vaid on tavaliselt lühipääsupunkti (nt ruuteri või võrgu lüli) aadress.

3: Anna kahebaidine raami tüübi väli kuueteistkümnendsüsteemis. Millisele kõrgema kihi protokollile see vastab?

- **Vihje:** Raami tüübi väli ütleb, millist tüüpi andmed Etherneti raami sees on. Näiteks, kui seal on IP andmed, siis vastab see protokollile IPv4.
- **Kuidas otsida:** Laienda Wiresharki aknas **Ethernet II** sektsioon ja leia väli **Type**. See on kahebaidine väli kuueteistkümnendsüsteemis. Otsi tüübi väärtust ja leia vastav protokoll (näiteks **0x0800** tähendab **IPv4**).

4: Mitu baiti alates Etherneti raami algusest asub ASCII “G” tähemärk sõnas GET?

- **Vihje:** Sõna "GET" on osa HTTP päringust, mis on kapseldatud TCP, IP ja Ethernet raami sees. Pead leidma, mitu baiti alates Etherneti raami algusest kulub selle sõnumini jõudmiseks.
- **Kuidas otsida:** Laienda **Ethernet II**, **IP**, **TCP** ja lõpuks **HTTP** sektsioonid Wiresharkis, kuni leiad sõna **GET**. Vaata, millisesse baiti see langeb (Wiresharki paketi detailide akna vasakul ääres on baiti järjekorrad). Arvuta, mitu baiti on Ethernet raami algusest kuni täheni "G".

---

2. Aadressilahendusprotokoll (ARP)

Selles osas jälgime **ARP protokolli** tegevuses. Soovitame enne jätkamist üle lugeda peatükk **6.4.1** tekstist.

ARP vahemälu (ARP caching)

ARP protokoll hoiab tavaliselt IP-aadresside ja Etherneti aadresside paare vahemälus. **ARP käsuga** (nii MSDOS-is kui ka Linuxis/Unixes) saab vaadata ja hallata selle vahemälu sisu. ARP protokoll ja ARP käsk võivad tunduda segadusse ajavad, kuid need on erinevad:

- **ARP protokoll** määrab, kuidas sõnumeid saadetakse ja vastu võetakse.
- **ARP käsk** võimaldab hallata ja vaadata ARP vahemälu sisu.

ARP vahemälu vaatamine:

1. **Windowsis**: Käivita MS-DOS käsurealt käsk **arp -a**, et näha ARP vahemälu sisu.

ARP vahemälu tühjendamine:

- **Windowsis**: Kasuta käsku **arp -d***, et tühjendada ARP vahemälu.

ARP tegevuses:

1. **ARP vahemälu tühjendamine**: Kasuta käske, et tühjendada ARP vahemälu.
2. **Jälgi ARP liiklust Wiresharkis**: Käivita Wireshark ja mine veebiaadressile:
   http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-lab-file3.html
   Lõpeta Wiresharki püük ja filtreeri välja kõrgema taseme protokollid, nii et näeksid ainult ARP ja Etherneti pakette.

Küsimused (ARP analüüsimiseks):

1: Mis on ARP taotluse Etherneti raamis allika ja sihtaadressid kuueteistkümnendsüsteemis?

- **Source (Allika) MAC-aadress:**
  Näide: **00:11:22:33:44:55**
  (See on sinu seadme MAC-aadress, mis saadab ARP taotluse.)
- **Destination (Sihtaadress):**
  Näide: **ff:ff:ff:ff:ff**

  (ARP taotlus on **broadcast**, seega läheb see kõigile seadmetele võrgus.)

2: Anna kahebaidine raami tüübi väärtus kuueteistkümnendsüsteemis. Millisele kõrgema kihi protokollile see vastab?

Ethernet raami tüübi väli:
Näide: **0x0806**
(See väärtus tähistab ARP protokolli. Kui näed seda, siis tead, et tegu on ARP sõnumiga.)

Küsimus 3: Laadi alla ARP spetsifikatsioon (https://www.rfc-editor.org/in-notes/std/std37.txt) ja vasta järgmistele küsimustele:

a) Mitu baiti alates Etherneti raami algusest asub ARP opcode väli?

- **ARP opcode väli asub** umbes **20. baidis** Etherneti raamist (see võib olla 20-22 baidi vahel, sõltuvalt sellest, kuidas arvestad päiseid).

b) Mis on opcode väli ARP taotluse raamis?

- **Opcode väärtus:**
  Näide: **1** (ARP taotlus)
  (See number tähistab, et tegu on ARP taotlusega. Kui oleks ARP vastus, oleks opcode väärtus **2**.)

c) Kas ARP sõnum sisaldab saatja IP-aadressi?

- **Sender IP Address (Saatja IP-aadress):**
  Näide: **192.168.1.10**
  (See on seadme IP-aadress, mis saadab ARP taotluse.)

d) Kus asub ARP taotluses "küsimus" – millise seadme MAC-aadressi jaoks IP-aadressi küsitakse?

- **Target IP Address (Küsimuse IP-aadress):**
  Näide: **192.168.1.1**
  (See on IP-aadress, mille jaoks MAC-aadressi küsitakse. ARP taotlus küsib, milline seade võrgus omab seda IP-aadressi.)

Wiresharkis näed neid väärtusi järgmiselt:

- **Ethernet II** sektsioonis on **Source** ja **Destination** MAC-aadressid.
- **Type** väli Ethernet II sektsioonis näitab raami tüüpi (ARP on **0x0806**).
- **ARP** sektsioonis näed **Opcode**, **Sender IP Address** ja **Target IP Address** välju.

Näiteks:

- **Ethernet II Source:** 00:11:22:33:44:55
- **Ethernet II Destination:** ff:ff:ff:ff:ff
- **Type:** 0x0806 (ARP)
- **ARP Opcode:** 1 (ARP Request)
- **ARP Sender IP Address:** 192.168.1.10
- **ARP Target IP Address:** 192.168.1.1

Need on näidised sellest, mida nad peaksid otsima ja milliseid numbreid Wiresharkis näha.