Laboratuvar Raporu 7

Eskişehir Osmangazi Üniversitesi

Bilgisayar Ağları

152116028

Özlem Kayıkcı

152120191043

Dr. Öğr. Üyesi İlker Özçelik

2022-2023

1 İçindekiler

2 Giriş

Bu laboratuvarda ethernet ve arp incelenmiş olup, yerel ağlarda (LAN) veri iletimi için kullanılan bir ağ teknolojisi olan Ethernet, Veri iletimi Ethernet'in frameleri adı verilen paketler aracılığıyla gerçekleşmektedir. Ethernet, fiziksel (MAC) adresler kullanarak cihazları tanımlar ve iletişim kurar ve kablolu bağlantılarla (örneğin Ethernet kablosu) genellikle kullanılan yaygın bir ağ protokolüdür.

ARP (Address Resolution Protocol), IP adreslerini (network katmanı) fiziksel (MAC) adreslere (düşük seviye ağ katmanı) çözmek için kullanılan bir ağ protokolüdür; ARP, IP adresi bilinen bir cihazın fiziksel adresini bulmak için kullanılmaktadır. Bir cihaz, ARP isteği yayınlayarak belirli bir IP adresine sahip cihazın MAC adresini öğrenmeye çalışır, ARP yanıtı da, hedef IP adresine sahip cihaza doğrudan gönderilir ve hedefin MAC adresini içermektedir. ARP, IP-MAC adreslerinin eşleştirmesini sağlayarak ağ iletişiminde paketlerin doğru hedefe yönlendirilmesini sağlamaktadır.

3 Laboratuvar Uygulaması

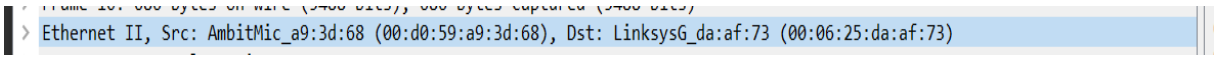
3.1 Ethernet ve ARP

No.	Time	Source	Destination	Protocol	Length	Info
1	20:19:20,157130	AmbitMic_a9:3d:68	Broadcast	ARP	42	Who has 192.168.1.1? Tell 192.168.1.105
2	20:19:20,158148	LinksysG_da:af:73	AmbitMic_a9:3d:68	ARP	60	192.168.1.1 is at 00:06:25:da:af:73
3	20:19:20,158158	192.168.1.105	199.2.53.206	TCP	62	1057 → 631 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM
4	20:19:23,119980	192.168.1.105	199.2.53.206	TCP	62	[TCP Retransmission] [TCP Port numbers reused] 1057 → 631 [SYN] Seq=0 Win=64240 Len=0
5	20:19:29,128618	192.168.1.105	199.2.53.206	TCP	62	[TCP Retransmission] [TCP Port numbers reused] 1057 → 631 [SYN] Seq=0 Win=64240 Len=0
6	20:19:33,700104	CnetTech_73:8d:ce	Broadcast	ARP	60	Who has 192.168.1.117? Tell 192.168.1.104
7	20:19:37,601553	192.168.1.105	128.119.245.12	TCP	62	1058 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM
8	20:19:37,623032	128.119.245.12	192.168.1.105	TCP	62	80 → 1058 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460 SACK_PERM
9	20:19:37,623057	192.168.1.105	128.119.245.12	TCP	54	1058 → 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0
10	20:19:37,623598	192.168.1.105	128.119.245.12	HTTP	686	GET /ethereal-labs/HTTP-ethereal-lab-file3.html HTTP/1.1
11	20:19:37,651896	128.119.245.12	192.168.1.105	TCP	60	80 → 1058 [ACK] Seq=1 Ack=633 Win=6952 Len=0
12	20:19:37,656065	128.119.245.12	192.168.1.105	TCP	1514	80 → 1058 [ACK] Seq=1 Ack=633 Win=6952 Len=1460 [TCP segment of a reassembled PDU]
13	20:19:37,657155	128.119.245.12	192.168.1.105	TCP	1514	80 → 1058 [ACK] Seq=1461 Ack=633 Win=6952 Len=1460 [TCP segment of a reassembled PDU]
14	20:19:37,657199	192.168.1.105	128.119.245.12	TCP	54	1058 → 80 [ACK] Seq=633 Ack=2921 Win=64240 Len=0
15	20:19:37,684187	128.119.245.12	192.168.1.105	TCP	1514	80 → 1058 [ACK] Seq=2921 Ack=633 Win=6952 Len=1460 [TCP segment of a reassembled PDU]
16	20:19:37,684552	128.119.245.12	192.168.1.105	HTTP	489	HTTP/1.1 200 OK (text/html)
17	20:19:37,684587	192.168.1.105	128.119.245.12	TCP	54	1058 → 80 [ACK] Seq=633 Ack=4816 Win=64240 Len=0

3.1.1 1.soru

1. What is the 48-bit Ethernet address of your computer?

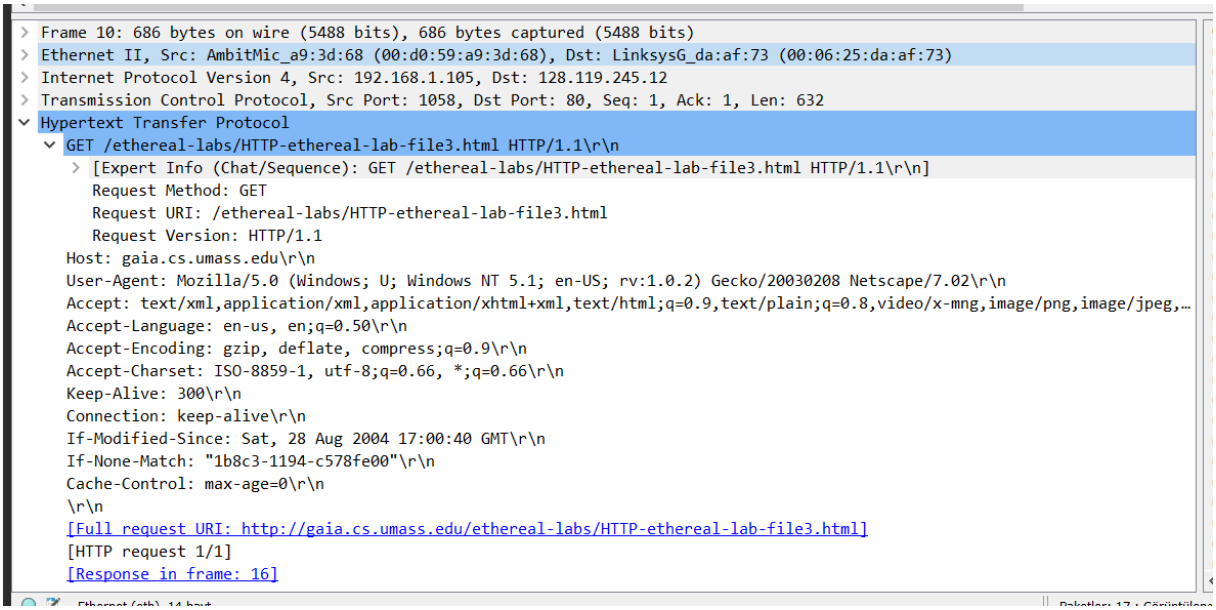
Bilgisayarımın Ethernet adresi wireshark ortamında ilgili trace izlenerek ekran görüntüsünde görüldüğü üzere 00:d0:59:a9:3d:68 olarak bulunmuştur.



3.1.2 2.soru

2. What is the 48-bit destination address in the Ethernet frame? Is this the Ethernet address of gaia.cs.umass.edu? (Hint: the answer is no). What device has this as its Ethernet address? [Note: this is an important question, and one that students sometimes get wrong. Re-read pages 468-469 in the text and make sure you understand the answer here.]

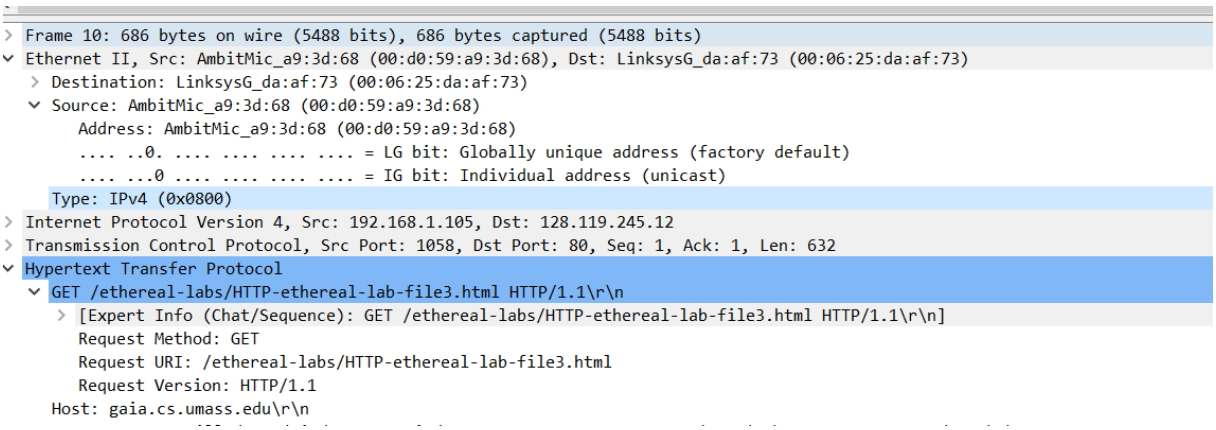
Destination adresi olan 00:06:25:da:af:73 adresi soruda belirlilen sitenin ethernet adresi değildir, Linksys yönlendirici/router'ın adresidir ve alt ağdan (subnet) çıkmak adına kullanılan bağlantının adresidir.



3.1.3 3.soru

3. Give the hexadecimal value for the two-byte Frame type field. What upper layer protocol does this correspond to?

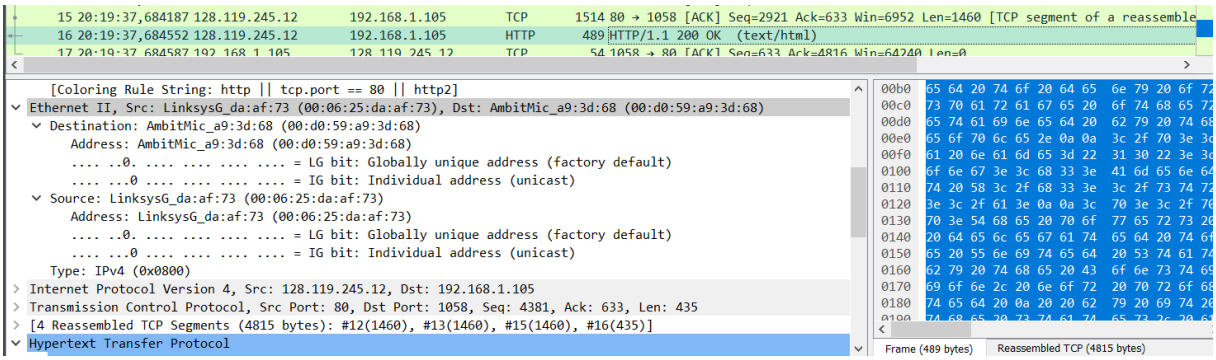
Ekran görüntüsünde görüldüğü üzere Type: IPv4 ve hex değeri olarak 0x0800 olarak bulunmuştur bu alan IP protokolüne karşılık gelmektedir yani frame type alanı ethernet frame'in payload'ının aktarılacağı IP'nin üstündeki katmana eş gelmektedir.



3.1.4 4.soru

4. How many bytes from the very start of the Ethernet frame does the ASCII “G” in “GET” appear in the Ethernet frame?

ASCII "G" harfi ekran görüntüsünde yer alan Ethernet çerçevesinin başlangıcından 52 byte uzaklıkta görünmektedir, 14 byte'lık bir Ethernet frame ve ardından 20 byte'lık bir IP header ile 20 byte'lık bir TCP header bulunmaktadır ve sonrasında da HTTP verileriyle karşılaşılmıştır.



3.1.5 5.soru

5. What is the value of the Ethernet source address? Is this the address of your computer, or of gaia.cs.umass.edu (Hint: the answer is no). What device has this as its Ethernet address?

Source adresi olan 00:06:25:da:af:73 adresi soruda belirlilen sitenin ethernet adresi değildir aynı zamanda benim bilgisayarımın adresi de değildir , bu adres Linksys yönlendirici/router’ın adresidir ve alt ağımdan (subnet) çıkmak adına kullanılan bağlantının adresidir.

3.1.6 6.soru

6. What is the destination address in the Ethernet frame? Is this the Ethernet address of your computer?

Destinasyon aresi olan 00:d0:59:a9:3d:68 adresi , bilgisayarımın Ethernet adresi olarak wireshark ortamında ilgili trace izlenerek bulunmuştur.

3.1.7 7.soru

7. Give the hexadecimal value for the two-byte Frame type field. What upper layer protocol does this correspond to?

İlgili alanda Type: IPv4 ve hex değeri olarak 0x0800 olarak bulunmuştur bu alan IP protokolüne karşılık gelmektedir yani sonuç olarak frame type alanı ethernet frame'in payload'ının aktarılacağı IP'nin üstündeki katmana denk geldiği görülmüştür.

3.1.8 8.soru

8. How many bytes from the very start of the Ethernet frame does the ASCII "O" in "OK" (i.e., the HTTP response code) appear in the Ethernet frame?

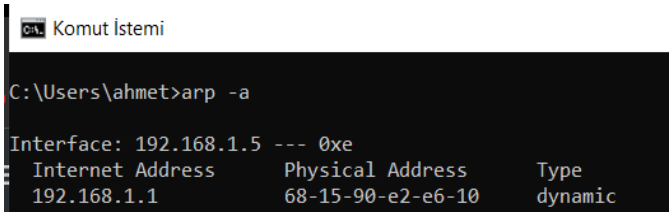
ASCII "O" harfi, Ethernet frame başlangıcından 52 byte uzaklıktadır, aynı şekilde 14 byte'lık bir Ethernet frame ve ardından 20 byte'lık bir IP header, 20 byte'lık bir TCP header gelir ve sonrasında HTTP verileriyle karşılaşılır.

3.2 The Address Resolution Protocol

3.2.1 9.soru

9. Write down the contents of your computer's ARP cache. What is the meaning of each column value?

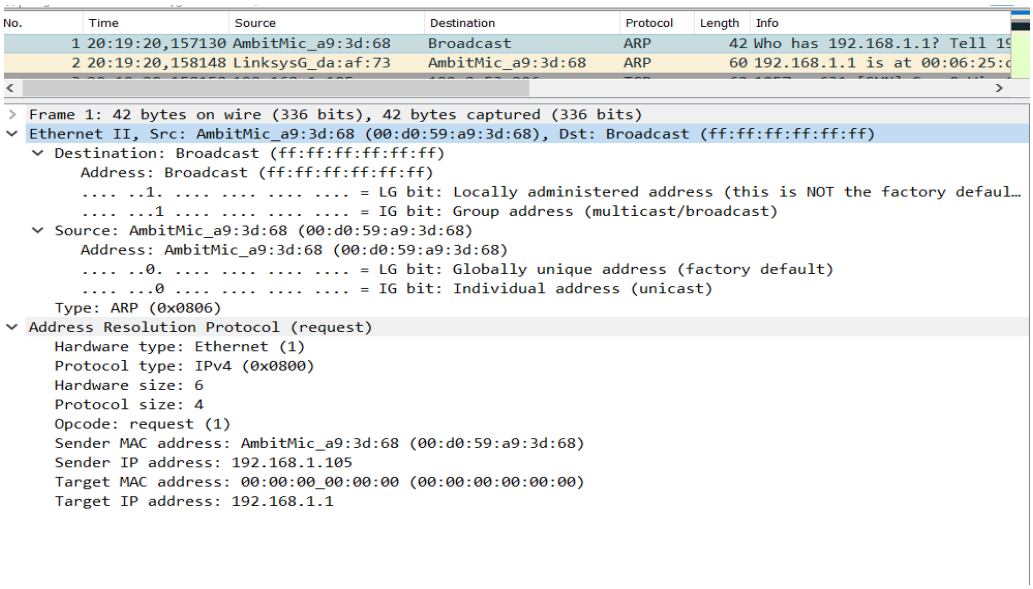
Internet Address sütunu IP adresini içermekte iken, Physical Address sütunu MAC adresini içermekte ve son olarak Type sütunu/alanı protokol türünü göstermektedir.



3.2.2 10.soru

10. What are the hexadecimal values for the source and destination addresses in the Ethernet frame containing the ARP request message?

Ethernet II için hexadecimal source adresi değeri 00:d0:59:a9:3d:68, ve destinasyon adresi değeri ff:ff:ff:ff:ff:ff olan Broadcast adresidir.



3.2.3 11.soru

11. Give the hexadecimal value for the two-byte Ethernet Frame type field. What upper layer protocol does this correspond to?

Hexadecimal değer olarak Ethernet Frame'in type alanı ARP için 0x0806 olarak ilgili trace izlendiğinde ekran görüntüsünde de gösterildiği üzere bulunmuştur.

3.2.4 12.soru

12. Download the ARP specification from ftp://ftp.rfc-editor.org/in-notes/std/std37.txt. A readable, detailed discussion of ARP is also at http://www.erg.abdn.ac.uk/users/gorry/course/inet-pages/arp.html.

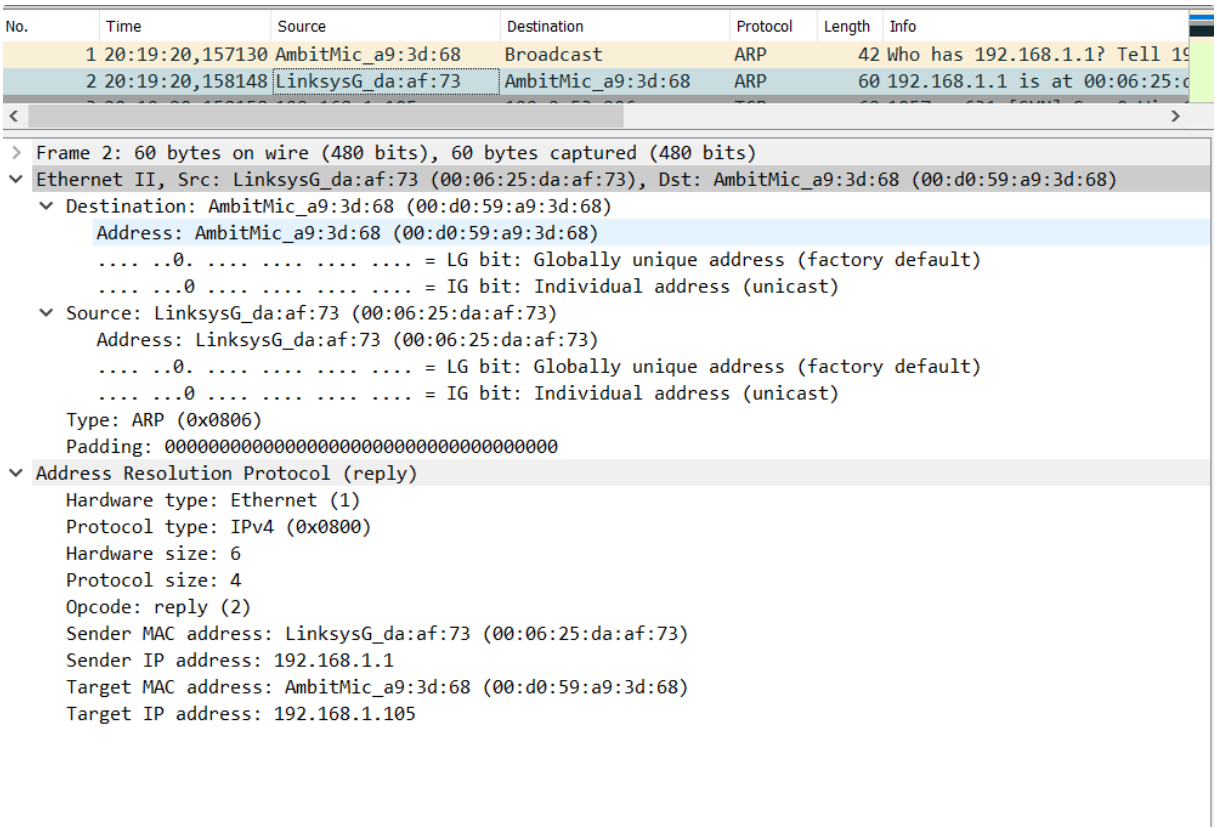
a) How many bytes from the very beginning of the Ethernet frame does the ARP opcode field begin?

b) What is the value of the opcode field within the ARP-payload part of the Ethernet frame in which an ARP request is made?

c) Does the ARP message contain the IP address of the sender?

d) Where in the ARP request does the "question" appear – the Ethernet address of the machine whose corresponding IP address is being queried?

a) Ethernet frame'in başlangıcına ,Arp opcode alanı 20 byte uzaklıktadır.
b) İstek mesajı için, ARP payload'ı (1) şeklinde gösterilmiş olup, 0x0001 'dir.
c) ARP mesajı gönderen için bir IP adresini taşımaktadır (sender) 192.168.1.1 olarak ekran görüntüsünde yer almaktadır.
d) "Target MAC address" alanı, sorgulanan IP adresine yani 192.168.1.1 adresine sahip olan makineye soru sormak için 00:00:00:00:00:00 olarak ayarlanmıştır.



3.2.5 13.soru

13. Now find the ARP reply that was sent in response to the ARP request.

a) How many bytes from the very beginning of the Ethernet frame does the ARP opcode field begin?

b) What is the value of the opcode field within the ARP-payload part of the Ethernet frame in which an ARP response is made?

c) Where in the ARP message does the "answer" to the earlier ARP request appear – the IP address of the machine having the Ethernet address whose corresponding IP address is being queried?

a) Ethernet frame'in başlangıcına ,Arp opcode alanı 20 byte uzaklıktadır.
b) Cevap (reply) mesajı için, ARP payload'ı (2) şeklinde gösterilmiş olup, 0x0002 'dir.
c) Önceki ARP request mesajımıza cevap sender MAC address kısmında yer almakta olup, IP adresi 192.168.1.1 olan gönderici için Ethernet adresi 00:06:25:da:af:73 olarak ekran görüntüsünde görülmektedir.

3.2.6 14.soru

14. What are the hexadecimal values for the source and destination addresses in the Ethernet frame containing the ARP reply message?

Source adresi için hexadecimal değer 00:06:25:da:af:73 ve destinasyon adresi için hexadecimal değer 00:d0:59:a9:3d:68 olarak ekran görüntüsünde gösterilmektedir.

3.2.7 15.soru

15. Open the ethernet-ethereal-trace-1 trace file in http://gaia.cs.umass.edu/wireshark-labs/wireshark-traces.zip. The first and second ARP packets in this trace correspond to an ARP request sent by the computer running Wireshark, and the ARP reply sent to the computer running Wireshark by the computer with the ARP-requested Ethernet address. But there is yet another computer on this network, as indicated by packet 6 – another ARP request. Why is there no ARP reply (sent in response to the ARP request in packet 6) in the packet trace?

İstek/request mesajının gönderildiği bilgisayarda olmadığımızdan izleme dosyası incelendiğinde herhangi bir reply mesajı yoktur ancak ARP isteği (request) yayınlanırken (broadcast), ARP yanıtı doğrudan gönderenin(sender) Ethernet adresine geri gönderilir.

4 Kaynakça

- Wireshark Lab: Ethernet and ARP v8.0 Supplement to Computer Networking: A Top-Down Approach, 8th ed., J.F. Kurose and K.W. Ross