CS 6043: Computer Networking

FALL 2017

PROJECT 3

Given: Nov. 15 (Wednesday), 2017

Due: Nov. 29 (Wednesday), 2017 (NO LATER THAN 11:59PM)

Members: Anshul Gautam and Chiranjivi Jawale

Submission Instructions:

1. Submit only on-line files on Blackboard before midnight. No hard copy will be accepted.

2. For students who are working in a team, *one* submission for the team is sufficient.

3. Wireshark files for this project can be found in the zip file "Project_3_Wireshark_Traces.zip".

Total possible points: 10

Part I: IP

Load the file 'IP_project_3.pcapng' in Wireshark and answer the following questions. The trace was generated while executing three *traceroute* commands with three different UDP datagram sizes (56, 2000, and 3000 bytes) on a computer with IP 10.63.7.60. The IP address of the target host was 103.74.84.13. Include screenshots in each case.

1.1 (0.5 pts) Select any of the ICMP echo packets from the trace. Within the IPv4 packet header, what is the value in the upper layer protocol field?

Answer:

ICMP – Protocol Number 1

```
> Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
  Total Length: 56
  Identification: 0xd5d0 (54736)
> Flags: 0x00
  Fragment offset: 0
  Time to live: 254
  Protocol: ICMP (1)
  Header checksum: 0xab58 [validation disabled]
  [Header checksum status: Unverified]
  Source: 10.32.32.1
  Destination: 10.63.7.60
```

1.2 (1 pts) Select any of the UDP packets generated from the second *traceroute* command. How many bytes are in the IP header? How many bytes are in the payload of the IP datagram? Explain how you determined the number of payload bytes.

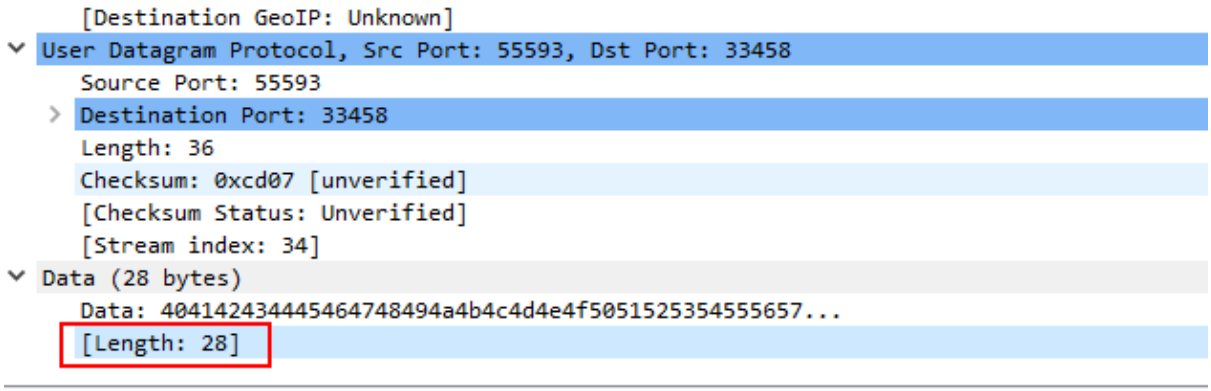
Answer:

56 bytes are present in IP header (20 bytes IP header + 8 bytes UDP header + 28 bytes of Payload). 36 bytes of payload is present in IP datagram (UDP header + payload).

```
74 2.699330 10.63.7.60          103.74.84.13          UDP
75 2.699336 10.63.7.60          103.74.84.13          UDP
76 2.699340 10.63.7.60          103.74.84.13          UDP
77 2.699344 10.63.7.60          103.74.84.13          UDP
78 2.699348 10.63.7.60          103.74.84.13          UDP
79 2.699352 10.63.7.60          103.74.84.13          UDP
80 2.699355 10.63.7.60          103.74.84.13          UDP
81 2.699359 10.63.7.60          103.74.84.13          UDP
82 2.699362 10.63.7.60          103.74.84.13          UDP
83 2.699379 10.63.7.60          103.74.84.13          UDP
84 2.699382 10.63.7.60          103.74.84.13          UDP

v Internet Protocol Version 4, Src: 10.63.7.60, Dst: 103.74.84.13
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 56
    Identification: 0x55e5 (21989)
  > Flags: 0x00
    Fragment offset: 0
    Time to live: 9
    Protocol: UDP (17)
    Header checksum: 0x8efe [validation disabled]
    [Header checksum status: Unverified]
    Source: 10.63.7.60
    Destination: 103.74.84.13
    [Source GeoIP: Unknown]
    [Destination GeoIP: Unknown]
v User Datagram Protocol, Src Port: 55593, Dst Port: 33458
    Source Port: 55593
```

The payload under UDP header is 28 bytes as seen in the snapshot

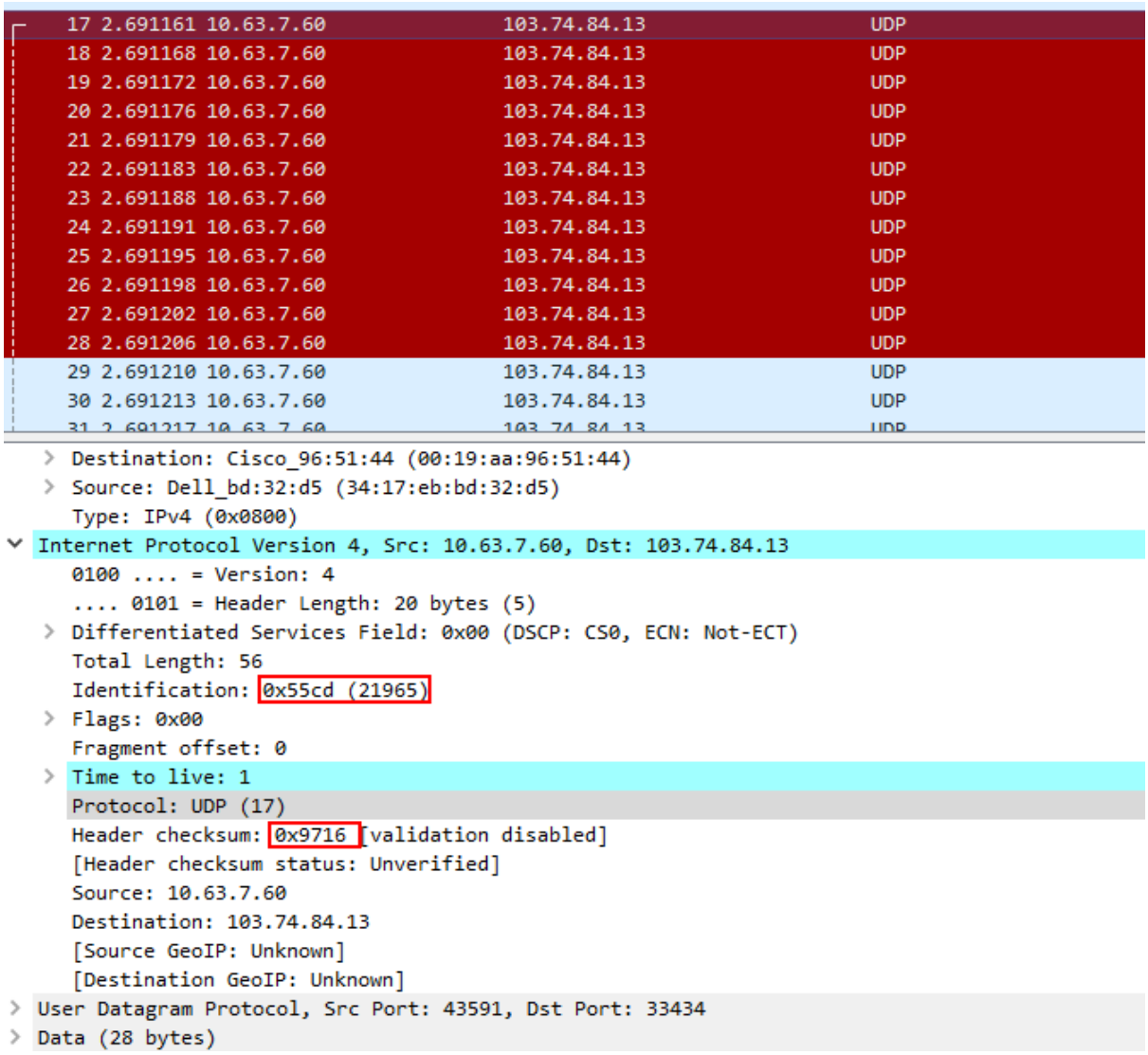


1.3 (0.5 pts) Observe the UDP packets generated from the first *traceroute* command. Which fields in the IP datagram always change from one datagram to the next within this series of messages sent by 10.63.7.60?

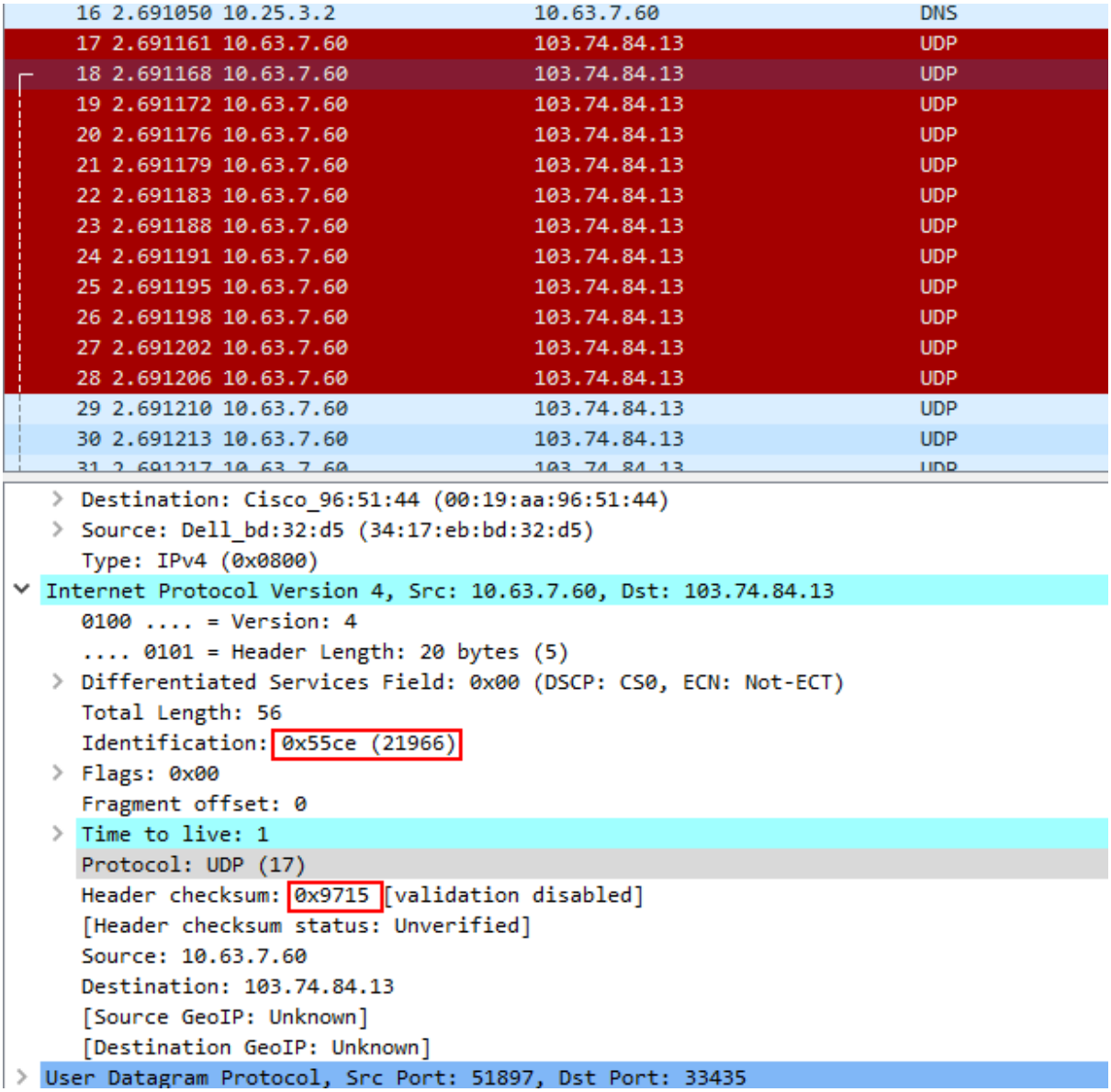
Answer:

Fields that changed between consecutive UDP packets include identification number. header checksum, and Time to Live (TTL). See snapshots

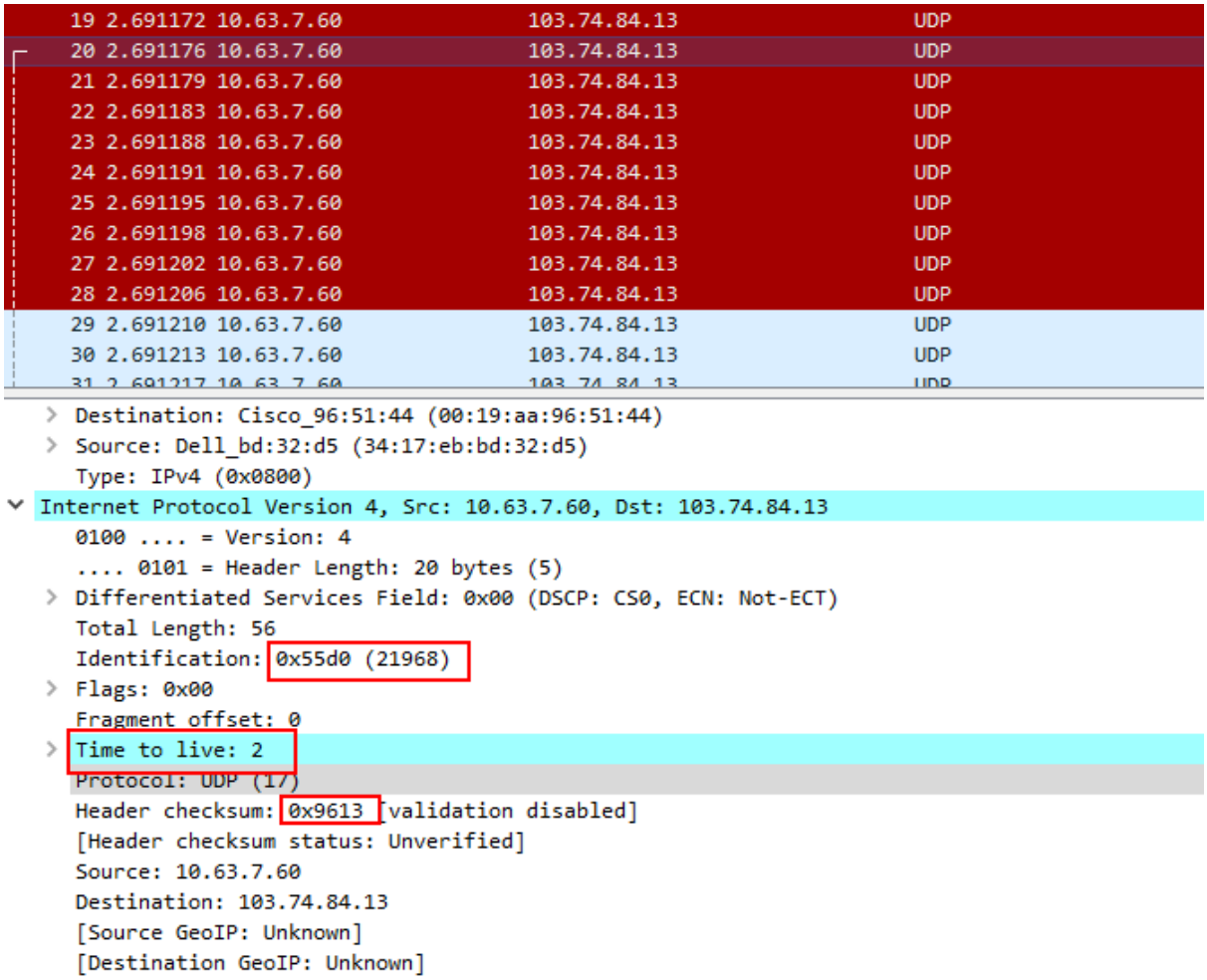
Packet number 17



Packet number 18



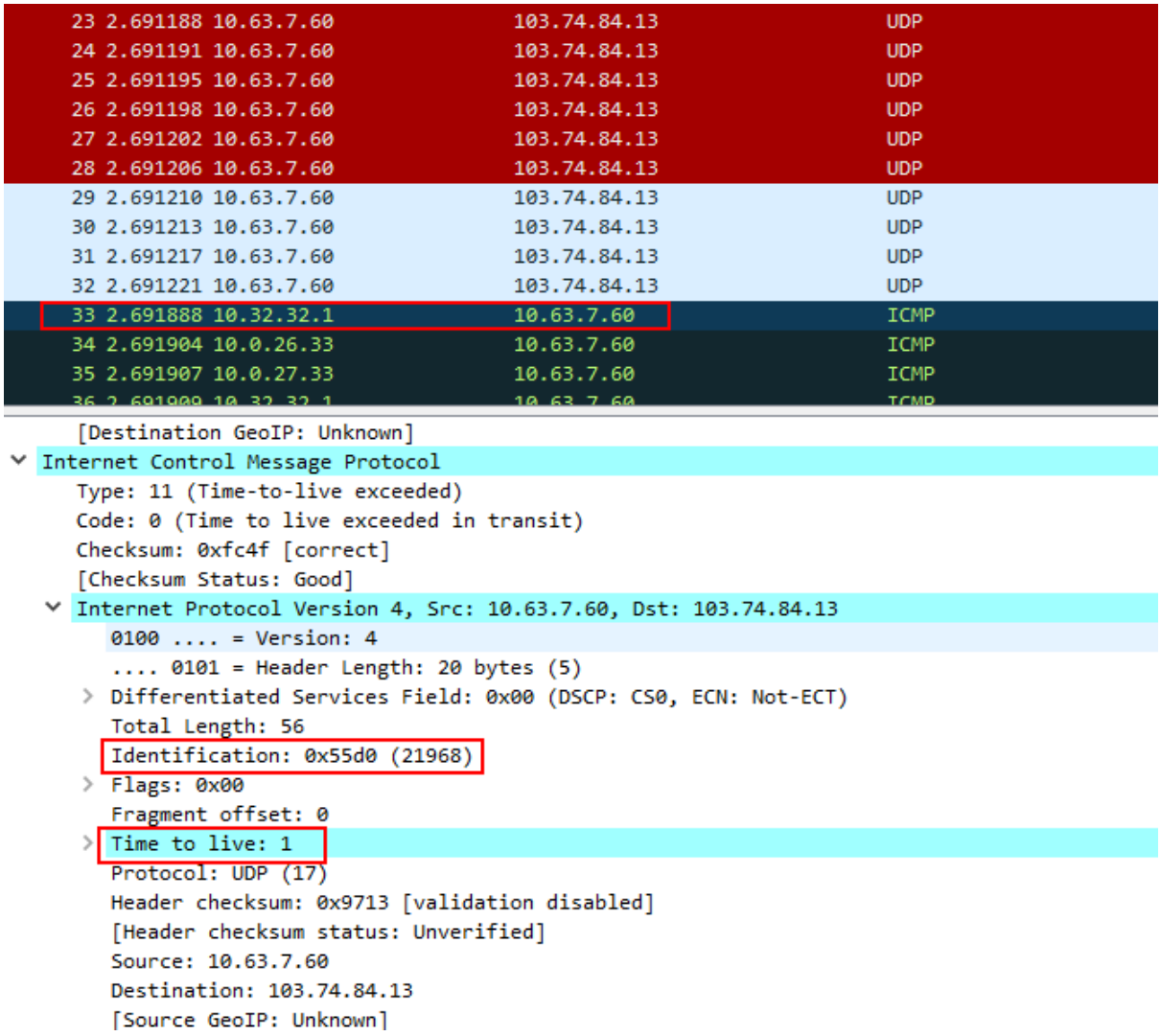
After every 3 UDP packets, the TTL increases by 1.



1.4 (1 pts) What is the value in the Identification field and the TTL field of the first ICMP packet (ping reply) received by 10.63.7.60?

Answer:

The value in identification field is 0x55d0 (21968) and TTL field is 1 as seen in the snapshot below.



Part II: DHCP

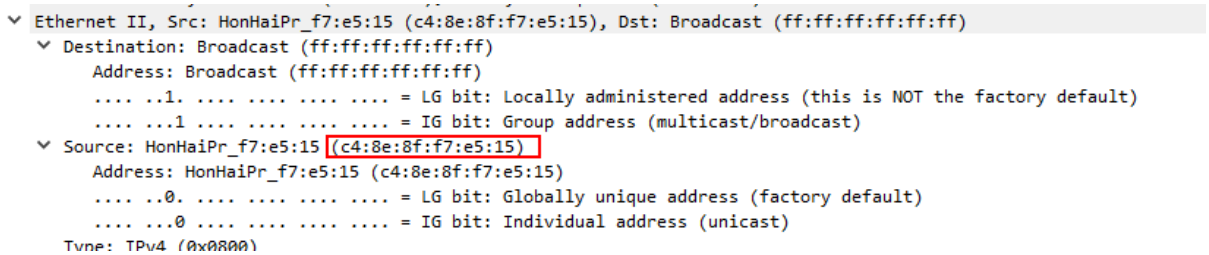
Load the file 'DHCP_project_3.pcapng' in Wireshark and answer the following questions. The trace was generated while releasing the host's current IP address and renewing it multiple times (Release → Renew → Renew → Release → Renew). Include screenshots in each case.

[Hint: Apply display filter "bootp" in Wireshark to filter out DHCP packets]

2.1 (0.5 pts) What is the link-layer address and the hardware address length of the host?

Answer:

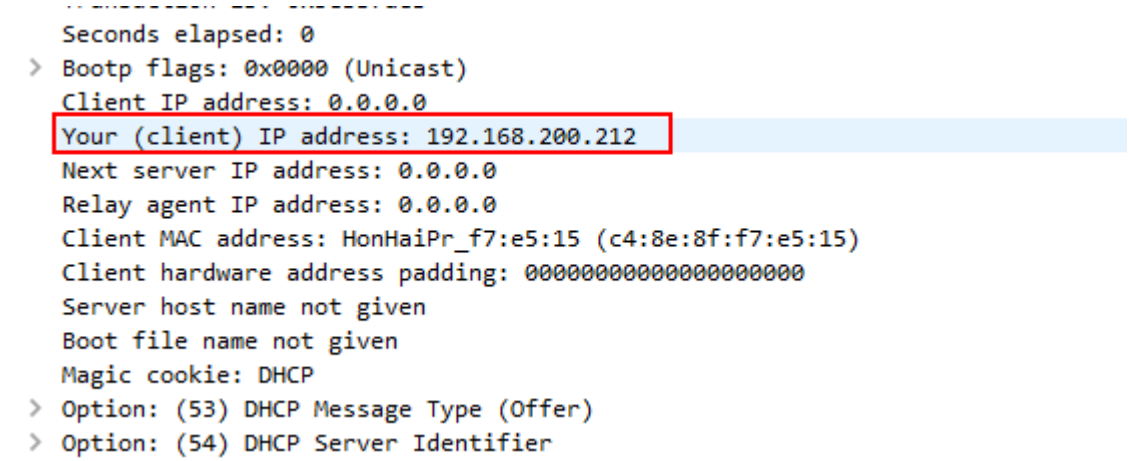
The MAC address length of the host is 48 bits and the address is c4:8e:8f:f7:e5:15.



2.2 (1 pts) What IP address is the DHCP server offering to your host in the first DHCP Offer message?

Answer:

192.168.200.212

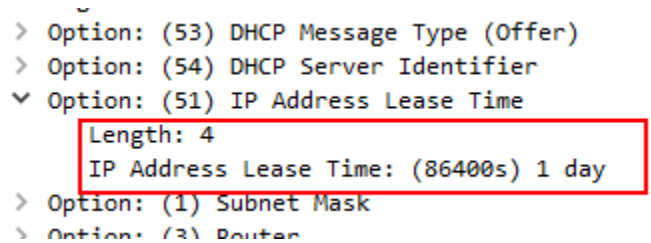


2.3 (1 pts) Explain the purpose of the lease time. How long is the lease time in your trace?

Answer:

Lease time is used by DHCP server to assign time for which the IP address can be used by the client. Once the lease time is over, the client needs to renew its IP address.

The IP address lease time offered by DHCP server is 86400s or 1 day.

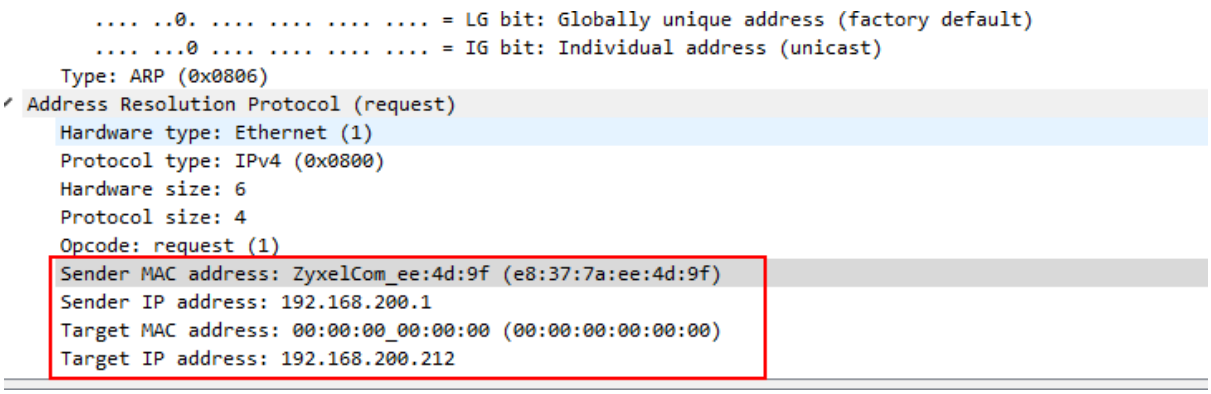


2.4 (1 pts) Clear the *bootp* display filter. Were any ARP packets sent or received in the trace? If so, explain the purpose of those ARP packets with a screenshotted example.

Answer:

The ARP request is sent by the DHCP server running on IP 192.168.200.1. Since the ARP request has both source and destination address, it looks like DHCP server want's to know if the IP address 192.168.200.212 is associated with the MAC address c4:8e:8f:f7:e5:15.

The same ARP request is sent 3 times but there is no ARP response which indicates to DHCP server that the IP address 192.168.200.212 doesn't belong to any interface.



Part III: Ethernet, ARP

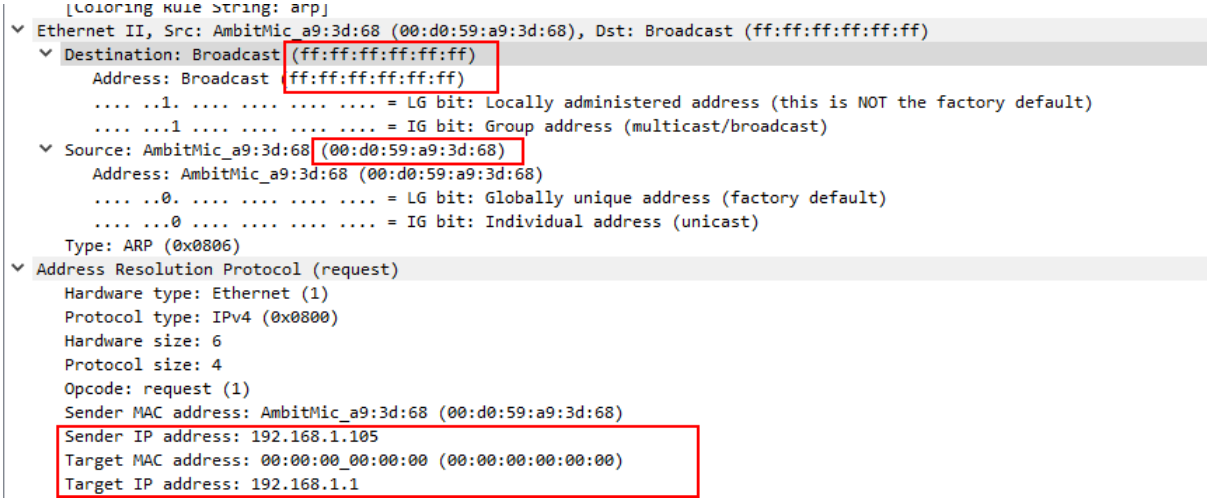
Load the file 'Eth_ARP_project_3.pcapng' in Wireshark and answer the following questions. The trace was generated while a web page was accessed (http://gaia.cs.umass.edu/wireshark-labs/HTTP-ethereal-lab-file3.html). Include screenshots in each case.

[Hint: For some of the questions, it might be helpful to disable IP or higher layer protocols. To do this, go to *Analyze->Enabled Protocols*]

3.1 (1 pts) What is the 48-bit destination address in the Ethernet frame? Is this the Ethernet address of gaia.cs.umass.edu? Explain why you answered yes or no.

Answer:

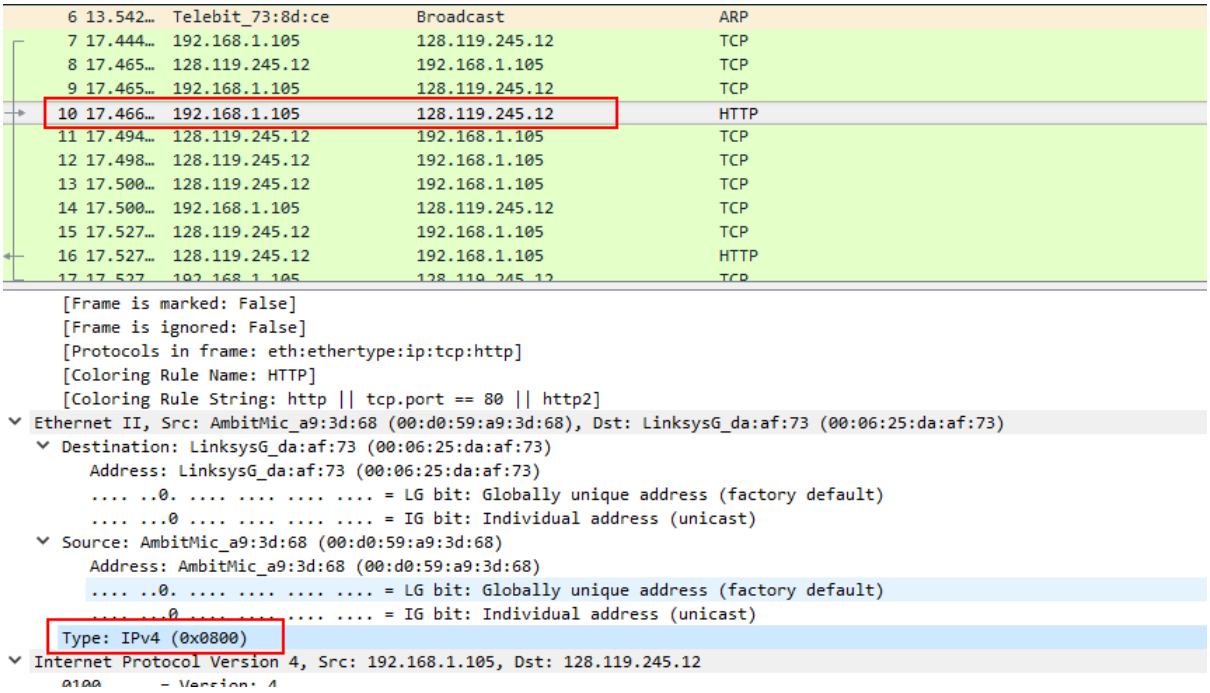
The first Ethernet frame is the ARP request sent by host with IP address 192.168.1.105 to destination IP address 192.168.1.1 which is the routers LAN interface address. The source MAC address in the Ethernet frame is 00:d0:59:a9:3d:68, and the destination is the broadcast address ff:ff:ff:ff:ff:ff as the source host doesn't know the MAC address of routers LAN interface. Once the host obtains the MAC address, it would send the Ethernet packet to the router and the packet would be routed to gaia.cs.umass.edu. The destination IP address in the ARP Ethernet frame doesn't belong to gaia.cs.umass.edu. It's the routers IP address. In order to connect with gaia.cs.umass.edu, the host needs routers MAC address to send the next TCP packet through the router and establish connection with gaia.cs.umass.edu.



3.2 (1 pts) Give the hexadecimal value for the two-byte 'frame type' field for frame number 10. What upper layer protocol does this correspond to?

Answer:

The upper layer protocol hex value is 0x800 and the corresponding upper layer protocol is IPv4.



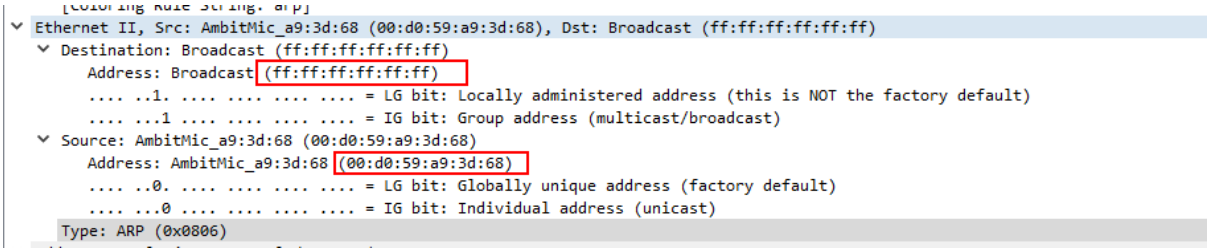
3.3 (0.5 pts) What are the hexadecimal values for the source and destination addresses in the Ethernet frame containing the ARP request message?

Answer:

The hexadecimal values for source and destination addresses in the Ethernet frame containing the ARP request message are the MAC addresses of the sending host and the broadcast.

Sending host: 00:d0:59:a9:3d:68

Broadcast: ff:ff:ff:ff:ff:ff



3.4 (1 pts) Does the ARP reply message contain the IP address of the requesting host? If yes, what is it?

Answer:

The ARP reply message contains the IP address of the requesting host. The IP address is 192.168.1.105.