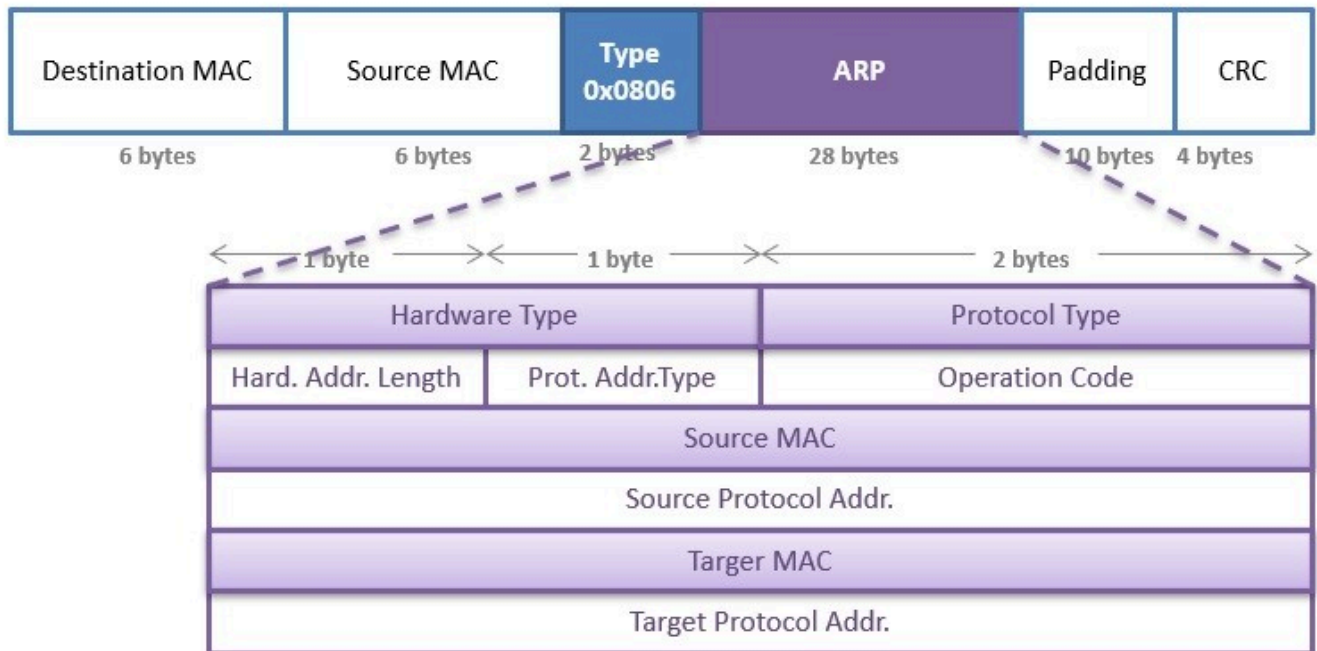


Assignment 2 wireshark

Q.1 How many bytes, from the very beginning of the Ethernet frame, does the ARP opcode field begin?

Ans - As from the diagram we can see that the total length of all the fields that exist before opcode field is 20 bytes i.e., Destination MAC (6 bytes) + Source MAC (6 bytes) + Type (2bytes) + Hardware Type (2 bytes) + Protocol Type (2 bytes) + Hardware Address Length (1 byte) + Protocol Address Type (1 byte) = 20 bytes. Thus the ARP opcode field begins after 20 bytes that is from the 21st byte from the very beginning of the Ethernet frame.



Q.2 What is the value of the opcode field within the ARP payload part of the Ethernet frame in which an ARP request is made?

Ans - The value in the opcode field within the ARP request payload part of the Ethernet frame is 1.

Below is the attached screenshot.

arp						
No.	Time	Source	Destination	Protocol	Length	Info
1170	6.306670	ServercomPri_15:b5:...	12:50:ce:9e:51:dc	ARP	42	Who has 192.168.1.5? Tell 192.168.1.1
1171	6.306694	12:50:ce:9e:51:dc	ServercomPri_15:b5:...	ARP	42	192.168.1.5 is at 12:50:ce:9e:51:dc


```
Frame 1170: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface \Device\NPF_{DD164123-9AD0-430E-8647-37AA3D32A742}, id 0
Ethernet II, Src: ServercomPri_15:b5:d8 (f0:ed:b8:15:b5:d8), Dst: 12:50:ce:9e:51:dc (12:50:ce:9e:51:dc)
Address Resolution Protocol (request)
  Hardware type: Ethernet (1)
  Protocol type: IPv4 (0x0800)
  Hardware size: 6
  Protocol size: 4
  Opcode: request (1)
    Sender MAC address: ServercomPri_15:b5:d8 (f0:ed:b8:15:b5:d8)
    Sender IP address: 192.168.1.1
    Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)
    Target IP address: 192.168.1.5
```

Q.3 Does the ARP message contain the IP address of the sender?

Ans - Yes the ARP message contains the IP address of the sender, below is the image proof attached.

```
Frame 1170: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface \Device\NPF_{DD164123-9AD0-430E-8647-37AA3D32A742}, id 0
Ethernet II, Src: ServercomPri_15:b5:d8 (f0:ed:b8:15:b5:d8), Dst: 12:50:ce:9e:51:dc (12:50:ce:9e:51:dc)
Address Resolution Protocol (request)
  Hardware type: Ethernet (1)
  Protocol type: IPv4 (0x0800)
  Hardware size: 6
  Protocol size: 4
  Opcode: request (1)
    Sender MAC address: ServercomPri_15:b5:d8 (f0:ed:b8:15:b5:d8)
    Sender IP address: 192.168.1.1
    Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)
    Target IP address: 192.168.1.5
```

Q.4 Wherein the ARP request, does the 'question' appear, that is, the Ethernet address of the machine whose corresponding IP address is being queried?

Ans - The **question** about the MAC address that the ARP request is querying from the corresponding IP address appears in the **Target MAC address** section of the ARP Payload part that is set to 00:00:00:00:00:00. Below is the attached screenshot for proof.

```
Frame 1170: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface \Device\NPF_{DD164123-9AD0-430E-8647-37AA3D32A742}, id 0
Ethernet II, Src: ServercomPri_15:b5:d8 (f0:ed:b8:15:b5:d8), Dst: 12:50:ce:9e:51:dc (12:50:ce:9e:51:dc)
Address Resolution Protocol (request)
  Hardware type: Ethernet (1)
  Protocol type: IPv4 (0x0800)
  Hardware size: 6
  Protocol size: 4
  Opcode: request (1)
    Sender MAC address: ServercomPri_15:b5:d8 (f0:ed:b8:15:b5:d8)
    Sender IP address: 192.168.1.1
    Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)
    Target IP address: 192.168.1.5
```

Q.5 How many bytes, from the very beginning of the Ethernet frame, does the ARP opcode field begin?

Ans - Same as answered in the first question.

Q.6 What is the value of the opcode field within the ARP payload part of the Ethernet frame in which an ARP request is made?

Ans - The value in the opcode field within the ARP reply payload part of the Ethernet frame is 2. Below is the attached screenshot.

```
▶ Frame 1171: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on  
▼ Ethernet II, Src: 12:50:ce:9e:51:dc (12:50:ce:9e:51:dc), Dst: ServercomP  
  ▶ Destination: ServercomPri_15:b5:d8 (f0:ed:b8:15:b5:d8)  
  ▶ Source: 12:50:ce:9e:51:dc (12:50:ce:9e:51:dc)  
    Type: ARP (0x0806)  
    [Stream index: 0]  
▼ Address Resolution Protocol (reply)  
  Hardware type: Ethernet (1)  
  Protocol type: IPv4 (0x0800)  
  Hardware size: 6  
  Protocol size: 4  
  Opcode: reply (2)  
  Sender MAC address: 12:50:ce:9e:51:dc (12:50:ce:9e:51:dc)  
  Sender IP address: 192.168.1.5  
  Target MAC address: ServercomPri_15:b5:d8 (f0:ed:b8:15:b5:d8)  
  Target IP address: 192.168.1.1
```

Q.7 Wherein the ARP message, does the 'answer' to the earlier ARP request appear, that is, the IP address of the machine having the Ethernet address whose corresponding IP address is being queried?

Ans - The about the MAC address that the ARP request is querying from the corresponding IP address appears in the section of the ARP reply Payload part. Below is the attached screenshot for proof.

```
Frame 1171: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on int  
Ethernet II, Src: 12:50:ce:9e:51:dc (12:50:ce:9e:51:dc), Dst: ServercomPri_1  
  ▶ Destination: ServercomPri_15:b5:d8 (f0:ed:b8:15:b5:d8)  
  ▶ Source: 12:50:ce:9e:51:dc (12:50:ce:9e:51:dc)  
    Type: ARP (0x0806)  
    [Stream index: 0]  
▼ Address Resolution Protocol (reply)  
  Hardware type: Ethernet (1)  
  Protocol type: IPv4 (0x0800)  
  Hardware size: 6  
  Protocol size: 4  
  Opcode: reply (2)  
  Sender MAC address: 12:50:ce:9e:51:dc (12:50:ce:9e:51:dc)  
  Sender IP address: 192.168.1.5  
  Target MAC address: ServercomPri_15:b5:d8 (f0:ed:b8:15:b5:d8)  
  Target IP address: 192.168.1.1
```