

Marc Soda
Ethernet and ARP lab

1. c4:41:1e:75:b1:52
2. 00:1e:c1:7e:d9:01
3. 0x0800 IPV4
4. Begins on the 67th Bit

```

# frame 120: 677 bytes on wire (544x8bits); 677 bytes captured (544x8bits) on interface emv, id 9
# Ethernet II, Src: BelkinIn_75:b3:52 (c4:c1:5e:75:b3:52), Dst: 3ComEuro_7e:09:01 (00:10:c1:7e:09:01)
+ Destination: 3ComEuro_7e:09:01 (00:10:c1:7e:09:01)
- Source: BelkinIn_75:b3:52 (c4:c1:5e:75:b3:52)
+ Address:BelkinIn_75:b3:52 (c4:c1:5e:75:b3:52)
... ..0..... = 1d bit: Globally unique address (factory default)
... ..1..... = 1E bit: Individual address (unicast)
Type: IPv4 (0x0800)
+ Internet Protocol Version 4, Src: 128.119.247.66, Dst: 128.119.245.12
+ Transmission Control Protocol, Src Port: 54842, Dst Port: 80, Seq: 1, Ack: 1, Len: 611
+ Hypertext Transfer Protocol

```

[illegible]

5. 00:1e:c1:7e:d9:01. No. It is the mac address of my router.
6. c4:41:1e:75:b1:52. Yes
7. 0x0800 IPV4
8. Starts on the 14th bit
9. 4

```

Frame 124: 583 bytes on wire (4664 bits), 583 bytes captured (4664 bits) on interface en0, id 0
Ethernet II, Src: XcomNetworks_78:1d:5d:08 (08:00:27:78:1d:5d:08), Dst: Belkinin_78:1d:5d:02 (08:00:27:78:1d:5d:02)
Destination: Belkinin_78:1d:5d:02 (08:00:27:78:1d:5d:02)
Source: XcomNetwork_7e:0d:01 (08:00:27:7e:0d:01)
Type: IPv4 (0x0008)
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 128.119.247.66
Transmission Control Protocol, Src Port: 80, Dst Port: 54482, Seq: 41414481, Len: 517
4 Resequence TCP Segments (4803 bytes)
Hypertext Transfer Protocol
  HTTP/1.2 200 OK
    [Expert Info (Chat/Sequence): HTTP/1.1 200 OK\r\n]
    Response Version: HTTP/1.1
    Status Code: 200
    [Status Code Description: OK]
    Content-Type: text/html
    Date: Tue, 02 Nov 2021 17:37:43 GMT\r\n
    Content-Length: 4508 bytes\r\n
    Last-Modified: Tue, 02 Nov 2021 05:59:02 GMT\r\n
    Etag: "1194-5c7cf7081a3a61"
    Accept-Ranges: bytes\r\n
    Connection: Keep-Alive\r\n
    Content-Length: 4508\r\n
    Keep-Alive: timeout=5, max=100\r\n
    Content-Type: text/html; charset=UTF-8\r\n\r\n
    HTTP response 1/2
    [Time since request: 0.001375060 seconds]
    [Request in frame: 124]
    [Next request in frame: 125]
    [Next response in frame: 124]
    Request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP/wireshark-lab-file1a.txt
    File data: 4508 bytes
  Line-based text: data:text/html (98 lines)

```

```

0000 48 54 54 54 71 65 26 31 20 32 30 32 30 32 06 06 HTTP/1.1 200 OK
0001 48 54 54 54 71 65 26 31 20 32 30 32 30 32 06 06   "text/css"
0002 70 29 29 29 29 29 29 29 29 29 29 29 29 29 29 29
0003 48 54 54 54 71 65 26 31 20 32 30 32 30 32 06 06
0004 68 68 68 68 68 68 68 68 68 68 68 68 68 68 68 68
0005 48 53 29 29 29 29 65 65 53 42 42 42 42 42 42 42
0006 68 68 68 68 68 68 68 68 68 68 68 68 68 68 68 68
0007 32 35 20 20 20 20 64 54 70 65 72 62 42 42 42 42
0008 68 68 68 68 68 68 68 68 68 68 68 68 68 68 68 68
0009 48 61 73 74 74 74 64 64 64 69 65 72 62 42 42 42
0010 54 75 65 65 65 65 65 65 65 65 65 65 65 65 65 65
0011 54 61 67 34 29 32 31 31 39 34 20 32 30 32 30 32
0012 64 38 38 38 38 38 38 38 38 38 38 38 38 38 38 38
0013 74 52 61 61 61 61 65 65 34 20 62 70 64 53 63 63
0014 43 67 64 64 64 64 64 64 64 64 64 64 64 64 64 64
0015 20 34 35 35 35 35 40 40 65 65 70 70 64 64 64 64
0016 65 34 20 34 35 35 35 67 75 74 30 30 30 30 30 30
0017 30 31 61 61 61 61 61 61 61 61 61 61 61 61 61 61
0018 20 34 35 40 65 65 65 65 41 61 69 70 65 64 64 64
0019 74 74 68 64 64 64 64 64 64 64 64 64 64 64 64 64
0020 74 74 68 64 64 64 64 64 64 64 64 64 64 64 64 64
0021 54 46 65 65 65 65 65 65 65 65 65 65 65 65 65 65
0022 65 61 64 26 26 26 34 74 69 74 65 65 65 65 65 65
0023 74 74 74 74 74 74 74 74 74 74 74 74 74 74 74 74
0024 48 74 54 54 48 45 20 40 40 44 44 20 40 40 40 40
0025 48 74 48 54 54 54 54 54 54 54 54 54 54 54 54 54
0026 61 61 61 61 61 61 61 61 61 61 61 61 61 61 61 61
0027 61 61 67 72 22 22 22 66 66 66 66 66 66 66 66 66
0028 61 61 61 61 61 61 61 61 61 61 61 61 61 61 61 61
0029 69 66 66 66 66 66 66 66 66 66 66 66 66 66 66 66
0030 66 66 66 66 66 66 66 66 66 66 66 66 66 66 66 66
0031 27 70 36 36 63 65 66 64 64 65 72 52 36 36 34 48
0032 40 40 42 40 42 40 42 40 42 40 42 40 42 40 42 40
0033 40 40 40 40 40 40 40 40 40 40 40 40 40 40 40 40

```

10. 1
11. Show mappings of internet addresses to physical addresses

```
marc@manray:~/working/screenshots$ arp -a
_ gateway (192.168.4.1) at 30:57:8e:b3:17:12 [ether] on wlan0
marc@manray:~/working/screenshots$
```

12. 00:1e:c1:7e:d9:01
13. ff:ff:ff:ff:ff:ff This address indicates that the message is a broadcast message. It does not correspond to a single device.
14. 0x0806 ARP
15. Begins on the 15th byte
16. 0001
17. Yes. 128.119.247.1
18. 128.119.247.77

```
Frame 1: 67 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface em0, id 0  
Ethernet II, Src: ScomEure7e:d9:01 (00:1c:c1:7e:d9:01), Dst: Broadcast (ff:ff:ff:ff:ff:ff)  
Internet Protocol Version 4, Src: ScomEure7e:d9:01 (00:1c:c1:7e:d9:01), Destination: 128.119.247.77  
Type: ARP (Request)  
+-----+  
| Trailer: 0x00000000000000000000000000000000 |  
+-----+  
Round-trip time: 0.000 seconds. Didn't find padding of zeros, and an unencoded trailer.  
  
Address Resolution Protocol (request)  
Hardware type: Ethernet (1)  
Protocol type: IPv4 (0x0800)  
Opcode size: 6  
Packet size: 4  
Opcode: request (1)  
Sender MAC address: ScomEure7e:d9:01 (00:1c:c1:7e:d9:01)  
Target MAC address: ff:ff:ff:ff:ff:ff (Broadcast)  
Source IP address: 128.119.247.77  
Target IP address: 128.119.247.77
```

```
0000 ff ff ff ff ff ff 00 1e c1 7e d9 01 08 05 00 01          00000000 00000000
0010 08 00 05 04 00 01 00 1e c1 7e d9 01 00 7f 01          00000000 00000000
0020 00 00 00 00 00 00 00 7f f7 4c 00 00 00 00 00          00000000 00000000
0030 00 00 00 00 00 00 00 00 20 20 20 20          00000000 00000000
```

20. 00:1e:c1:7e:d9:01

21. These are broadcast messages. The response was sent back to the appropriate device, not my device.