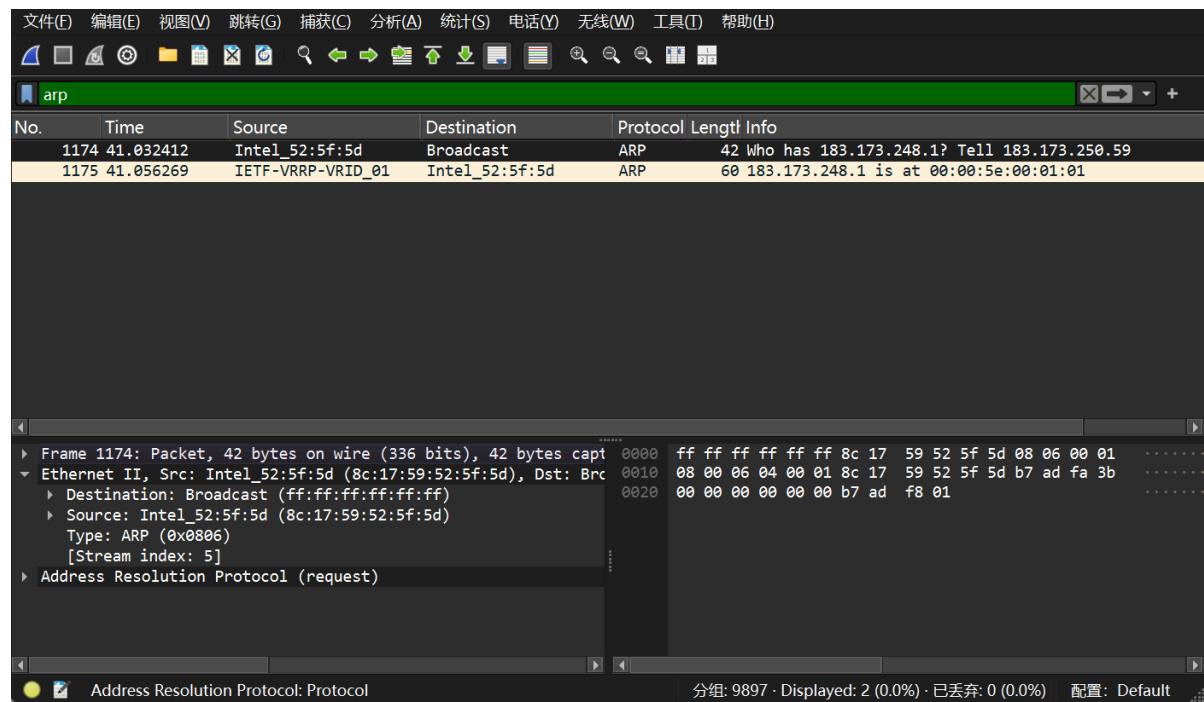


第二次实验报告

张峰源 2023010859

实验题目

(1) ARP协议在以太网帧头中载荷类型的编号是?



0x0806

(2) ARP分组头中，以太网硬件类型编号和IP协议类型编号分别是？

```
▼ Address Resolution Protocol (request)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: request (1)
    Sender MAC address: Intel_52:5f:5d (8c:17:59:52:5f:5d)
    Sender IP address: 183.173.250.59
    Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)
    Target IP address: 183.173.248.1
```

硬件类型编号：Ethernet (1)

IP协议类型编号：IPv4 (0x0800)

(3) ARP请求分组中，操作码（Opcode）值是？源IP地址及MAC地址，目的IP地址及MAC地址是多少？

```
► Ethernet II, Src: Intel_52:5f:5d (8c:17:59:52:5f:5d), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
▼ Address Resolution Protocol (request)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: request (1)
    Sender MAC address: Intel_52:5f:5d (8c:17:59:52:5f:5d)
    Sender IP address: 183.173.250.59
    Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)
    Target IP address: 183.173.248.1
```

No.	0000	0010	0020	Length	Hex	Dec	Description
1174	ff ff ff ff ff 8c 17 59 52 5f 5d 08 06 00 01	08 00 06 04 00 01 8c 17 59 52 5f b7 ad fa 3b	00 00 00 00 00 00 b7 ad f8 01	42 YR_] YR_]	

No.: 1174 · Time: 41.032412 · Source: Intel_52:5f:5d · Desti...ength: 42 · Info: Who has 183.173.248.1? Tell 183.173.250.59

Show packet bytes Layout: Vertical (Stacked) ▾

关闭 帮助

操作码: request (1)

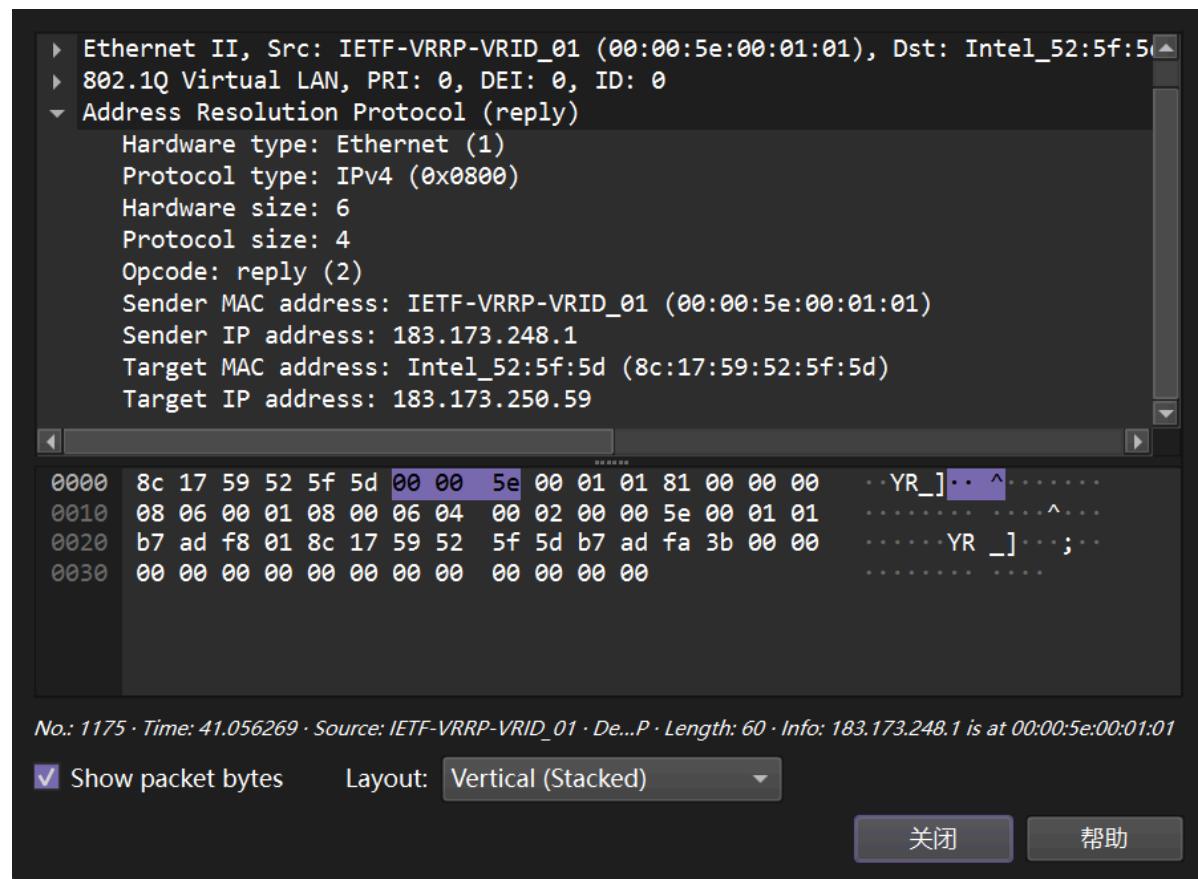
源IP地址: 183.173.250.59

源MAC地址: Intel_52:5f:5d(8c:17:59:52:5f:5d)

目的IP地址: 183.173.248.1

目的MAC地址: 00: 00: 00_00: 00: 00

(4) ARP回复分组中，操作码 (Opcode) 值是？源IP地址及MAC地址，目的IP地址及MAC地址是多少？



操作码: reply (2)

源IP地址: 183.173.248.1

源MAC地址: IETF-VRRP-VRID_01 (00:00:5e:00:01:01)

目的IP地址: 183.173.250.59

目的MAC地址：Intel_52:5f:5d(8c:17:59:52:5f:5d)

简述题

(1) ping 同一局域网内的主机和局域网外的主机，都会产生 ARP 报文么？所产生的 ARP 报文有何不同，为什么？

答：都会产生。ping 局域网内主机时，ARP 请求目标主机的 MAC；ping 外网主机时，ARP 仅请求网关的 MAC。因为外网通信需经网关转发，主机无需知晓外网主机 MAC，仅需网关 MAC 即可完成数据转发。

(2) ARP 请求数据包是支撑 TCP/IP 协议正常运作的广播包。如果滥发或错发 ARP 广播包会产生哪些不良影响？如何发现和应对？

答：大量广播会导致网络拥堵、进行 ARP 欺骗、主机通信失败。可用wireshark监控，配置静态 ARP 表、开启设备 ARP 防护、部署 IDS 检测异常报文来进行应对。