

# Wireshark抓包实验-2

1.

EtherType = 0x0806

```
▶ Frame 1760: Packet, 42 bytes on wire (336 bits), 42 bytes captured (336 bits)
└─ Ethernet II, Src: Intel_73:1b:bc (ec:4c:8c:73:1b:bc), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
    └─ Destination: Broadcast (ff:ff:ff:ff:ff:ff)
    └─ Source: Intel_73:1b:bc (ec:4c:8c:73:1b:bc)
    └─ Type: ARP (0x0806)
        [Stream index: 5]
▶ Address Resolution Protocol (request)
```

2.

Hardware type (HTYPE · 以太网) = 1 Protocol type (PTYPE, IPv4) = 0x0800

```
└─ 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_73:1b:bc (ec:4c:8c:73:1b:bc)
    └─ Sender IP address: 183.173.247.112
    └─ Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)
    └─ Target IP address: 183.173.240.1
```

3.

Opcode = 1 (request) 源 IP 183.173.247.112 源 MAC ec:4c:8c:73:1b:bc 目的 IP 183.173.240.1 目的 MAC 00:00:00:00:00:00

```
└─ 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_73:1b:bc (ec:4c:8c:73:1b:bc)
    └─ Sender IP address: 183.173.247.112
    └─ Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)
    └─ Target IP address: 183.173.240.1
```

4.

Opcode = 2 (reply) 源 IP 183.173.240.1 源 MAC 00:00:5e:00:01:01 目的 IP 183.173.247.112 目的 MAC ec:4c:8c:73:1b:bc

▼ Address Resolution Protocol (reply)

- Hardware type: Ethernet (1)
- Protocol type: IPv4 (0x0800)
- Hardware size: 6
- Protocol size: 4
- Opcode: reply (2)
- Sender MAC address: IETF-VRP-VRID\_01 (00:00:5e:00:01:01)
- Sender IP address: 183.173.240.1
- Target MAC address: Intel\_73:1b:bc (ec:4c:8c:73:1b:bc)
- Target IP address: 183.173.247.112

简述题 (1)

会。局域网内 ping : ARP 解析的是目标主机 IP→MAC；局域网外 ping : ARP 解析的是默认网关 IP→MAC。因为 ARP 只在本链路解析“下一跳”的 MAC，跨网段必须先发给网关。

(2)

影响：广播风暴占带宽/CPU；ARP 表被污染导致断网/错投递；可被用于 ARP 欺骗/中间人/DoS。发现：Wireshark/arpwatch 看到异常频率或 IP-MAC 频繁变更。应对：隔离异常主机、清 ARP 缓存、静态 ARP；交换机启用 DHCP Snooping + DAI、端口安全、限速与分 VLAN。

## Wireshark 抓包实验-3

---

### 抓包实验1：观察IPv4包与分段现象

▼ Internet Protocol Version 4, Src: 8.209.237.49, Dst: 183.173.247.111

- 0100 .... = Version: 4
- .... 0101 = Header Length: 20 bytes (5)
- Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
- Total Length: 242
- Identification: 0xb1fa (45562)
- 010. .... = Flags: 0x2, Don't fragment
- ...0 0000 0000 0000 = Fragment Offset: 0
- Time to Live: 45
- Protocol: TCP (6)
- Header Checksum: 0xf5ea [validation disabled]
- [Header checksum status: Unverified]

Version = 4 IHL = 5 IHL 单位：32-bit word (4字节) · 所以  $5 \times 4 = 20$  字节头部

(1)

854402	4356.218203	183.173.247.112	182.61.200.108	ICMP
•	855391	4361.219536	183.173.247.112	182.61.200.108
•	855392	4361.219536	183.173.247.112	182.61.200.108
•	855393	4361.219536	183.173.247.112	182.61.200.108
<pre>▶ Frame 855393: Packet, 82 bytes on wire (656 bits), 82 bytes captured ▶ Ethernet II, Src: Intel_73:1b:bc (ec:4c:8c:73:1b:bc), Dst: IETF-VRRP-   ▶ Internet Protocol Version 4, Src: 183.173.247.112, Dst: 182.61.200.10     0100 .... = Version: 4     .... 0101 = Header Length: 20 bytes (5)   ▶ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)     Total Length: 68     Identification: 0x41ec (16876)   ▶ 000. .... = Flags: 0x0     ...0 0001 0111 0010 = Fragment Offset: 2960     Time to Live: 128     Protocol: ICMP (1)     Header Checksum: 0x0000 [validation disabled]       [Header checksum status: Unverified]     Source Address: 183.173.247.112     Destination Address: 182.61.200.108   ▶ [3 TPv4 Fragments (3008 bytes): #855391(1480). #855392(1480). #855393(1480)]</pre>				
855391	4361.219536	183.173.247.112	182.61.200.108	IPv4
855392	4361.219536	183.173.247.112	182.61.200.108	IPv4
•	855393	4361.219536	183.173.247.112	182.61.200.108
<pre>▶ Frame 855392: Packet, 1514 bytes on wire (12112 bits), 1514 bytes captured ▶ Ethernet II, Src: Intel_73:1b:bc (ec:4c:8c:73:1b:bc), Dst: IETF-VRRP-   ▶ Internet Protocol Version 4, Src: 183.173.247.112, Dst: 182.61.200.10     0100 .... = Version: 4     .... 0101 = Header Length: 20 bytes (5)   ▶ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)     Total Length: 1500     Identification: 0x41ec (16876)   ▶ 001. .... = Flags: 0x1, More fragments     ...0 0000 1011 1001 = Fragment Offset: 1480     Time to Live: 128     Protocol: ICMP (1)     Header Checksum: 0x0000 [validation disabled]       [Header checksum status: Unverified]</pre>				

854401	4356.218203	183.173.247.112	182.61.200.108	IPv4
854402	4356.218203	183.173.247.112	182.61.200.108	ICMP
855391	4361.219536	183.173.247.112	182.61.200.108	IPv4
855392	4361.219536	183.173.247.112	182.61.200.108	IPv4
• 855393	4361.219536	183.173.247.112	182.61.200.108	ICMP

► Frame 855391: Packet, 1514 bytes on wire (12112 bits), 1514 bytes captured

► Ethernet II, Src: Intel\_73:1b:bc (ec:4c:8c:73:1b:bc), Dst: IETF-VRRP-  
    0100 .... = Version: 4  
    .... 0101 = Header Length: 20 bytes (5)

► Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)  
    Total Length: 1500  
    Identification: 0x41ec (16876)

► 001. .... = Flags: 0x1, More fragments  
    ...0 0000 0000 0000 = Fragment Offset: 0  
    Time to Live: 128  
    Protocol: ICMP (1)  
    Header Checksum: 0x0000 [validation disabled]  
    [Header checksum status: Unverified]

相等，都是0x41ec

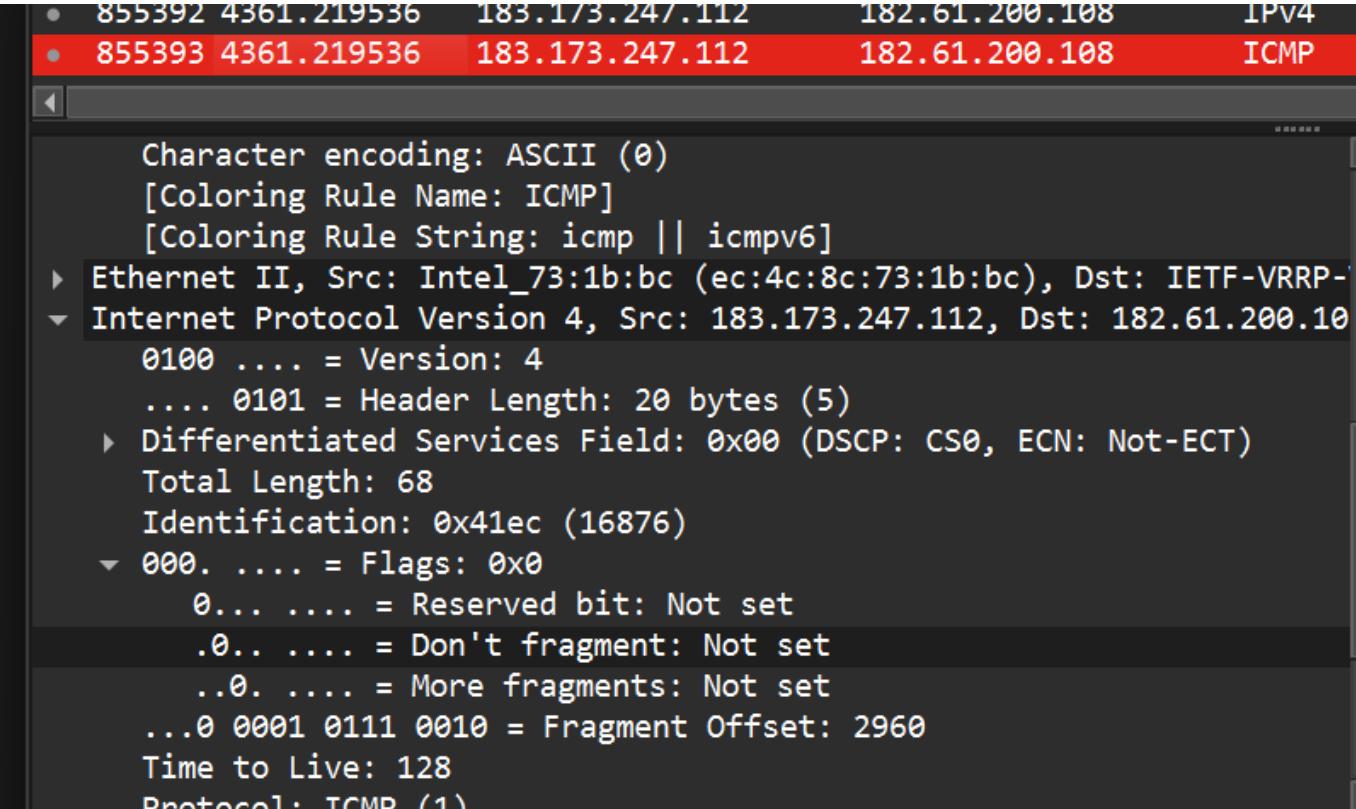
(2)

854401	4356.218203	183.173.247.112	182.61.200.108	IPv4
854402	4356.218203	183.173.247.112	182.61.200.108	ICMP
855391	4361.219536	183.173.247.112	182.61.200.108	IPv4
855392	4361.219536	183.173.247.112	182.61.200.108	IPv4
•	855393	4361.219536	183.173.247.112	182.61.200.108
<b>Character encoding: ASCII (0)</b>				
►	Ethernet II, Src: Intel_73:1b:bc (ec:4c:8c:73:1b:bc), Dst: IE			
▼	Internet Protocol Version 4, Src: 183.173.247.112, Dst: 182.6			
0100 .... = Version: 4				
.... 0101 = Header Length: 20 bytes (5)				
► Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-E)				
Total Length: 1500				
Identification: 0x41ec (16876)				
▼ 001. .... = Flags: 0x1, More fragments				
0... .... = Reserved bit: Not set				
.0.. .... = Don't fragment: Not set				
..1. .... = More fragments: Set				
...0 0000 0000 0000 = Fragment Offset: 0				
Time to Live: 128				
Protocol: ICMP (1)				
854401	4356.218203	183.173.247.112	182.61.200.108	IPv4
854402	4356.218203	183.173.247.112	182.61.200.108	ICMP
855391	4361.219536	183.173.247.112	182.61.200.108	IPv4
855392	4361.219536	183.173.247.112	182.61.200.108	IPv4
•	855393	4361.219536	183.173.247.112	182.61.200.108
<b>Character encoding: ASCII (0)</b>				
►	Ethernet II, Src: Intel_73:1b:bc (ec:4c:8c:73:1b:bc), Dst: IETF-VRRP-			
▼	Internet Protocol Version 4, Src: 183.173.247.112, Dst: 182.61.200.10			
0100 .... = Version: 4				
.... 0101 = Header Length: 20 bytes (5)				
► Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)				
Total Length: 1500				
Identification: 0x41ec (16876)				
▼ 001. .... = Flags: 0x1, More fragments				
0... .... = Reserved bit: Not set				
.0.. .... = Don't fragment: Not set				
..1. .... = More fragments: Set				
...0 0000 1011 1001 = Fragment Offset: 1480				
Time to Live: 128				
Protocol: ICMP (1)				
Header Checksum: 0x0000 [validation disabled]				
[Header checksum status: Unverified]				

DF=0 : 允许分片

MF=1 : 后面还有分片

(3)



Character encoding: ASCII (0)  
[Coloring Rule Name: ICMP]  
[Coloring Rule String: icmp || icmpv6]

► Ethernet II, Src: Intel\_73:1b:bc (ec:4c:8c:73:1b:bc), Dst: IETF-VRRP-  
▼ Internet Protocol Version 4, Src: 183.173.247.112, Dst: 182.61.200.10  
    0100 .... = Version: 4  
    .... 0101 = Header Length: 20 bytes (5)  
    ► Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)  
        Total Length: 68  
        Identification: 0x41ec (16876)  
    ▼ 000. .... = Flags: 0x0  
        0.... .... = Reserved bit: Not set  
        .0... .... = Don't fragment: Set  
        ..0. .... = More fragments: Set  
        ...0 0001 0111 0010 = Fragment Offset: 2960  
        Time to Live: 128  
        Protocol: TCPMP (1)

DF=0 : 允许分片 MF=0 : 这是最后一个分片

(4)

854402 4356.218203	183.173.247.112	182.61.200.108	IPv4
855391 4361.219536	183.173.247.112	182.61.200.108	IPv4
855392 4361.219536	183.173.247.112	182.61.200.108	IPv4
• 855393 4361.219536	183.173.247.112	182.61.200.108	IPv4

Character encoding: ASCII (0)

► Ethernet II, Src: Intel\_73:1b:bc (ec:4c:8c:73:1b:bc), Dst: IETF-VRRP (08:00:00:00:00:00) (oui-registered)  
▼ Internet Protocol Version 4, Src: 183.173.247.112, Dst: 182.61.200.108  
    0100 .... = Version: 4  
    .... 0101 = Header Length: 20 bytes (5)  
    ► Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)  
        Total Length: 1500  
        Identification: 0x41ec (16876)  
    ▼ 001. .... = Flags: 0x1, More fragments  
        0... .... = Reserved bit: Not set  
        .0.. .... = Don't fragment: Not set  
        ..1. .... = More fragments: Set  
        ...0 0000 0000 0000 = Fragment Offset: 0  
        Time to Live: 128  
        Protocol: ICMP (1)  
Header Checksum: 0x0000 [validation disabled]  
Header checksum status: Unverified

854401 4356.218203	183.173.247.112	182.61.200.108	IPv4
854402 4356.218203	183.173.247.112	182.61.200.108	ICMP
855391 4361.219536	183.173.247.112	182.61.200.108	IPv4
855392 4361.219536	183.173.247.112	182.61.200.108	IPv4
• 855393 4361.219536	183.173.247.112	182.61.200.108	ICMP

Character encoding: ASCII (0)

► Ethernet II, Src: Intel\_73:1b:bc (ec:4c:8c:73:1b:bc), Dst: IETF-VRRP (08:00:00:00:00:00) (oui-registered)  
▼ Internet Protocol Version 4, Src: 183.173.247.112, Dst: 182.61.200.108  
    0100 .... = Version: 4  
    .... 0101 = Header Length: 20 bytes (5)  
    ► Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)  
        Total Length: 1500  
        Identification: 0x41ec (16876)  
    ▼ 001. .... = Flags: 0x1, More fragments  
        0... .... = Reserved bit: Not set  
        .0.. .... = Don't fragment: Not set  
        ..1. .... = More fragments: Set  
        ...0 0000 1011 1001 = Fragment Offset: 1480  
        Time to Live: 128  
        Protocol: ICMP (1)  
Header Checksum: 0x0000 [validation disabled]  
Header checksum status: Unverified

```

• 855392 4361.219536 183.173.247.112 182.61.200.108 IPv4
• 855393 4361.219536 183.173.247.112 182.61.200.108 ICMP

Character encoding: ASCII (0)
[Coloring Rule Name: ICMP]
[Coloring Rule String: icmp || icmpv6]
Ethernet II, Src: Intel_73:1b:bc (ec:4c:8c:73:1b:bc), Dst: IETF-VRRP
Internet Protocol Version 4, Src: 183.173.247.112, Dst: 182.61.200.108
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
    ▶ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
        Total Length: 68
        Identification: 0x41ec (16876)
    ▼ 000. .... = Flags: 0x0
        0.... .... = Reserved bit: Not set
        .0.. .... = Don't fragment: Not set
        ..0. .... = More fragments: Not set
        ...0 0001 0111 0010 = Fragment Offset: 2960
        Time to Live: 128
        Protocol: ICMP (1)

```

分片1 offset = 0

分片2 offset = 1480

分片3 offset = 1480+1480 = 2960

(5) 因为 ping -l 3000 指的是 ICMP 数据部分 3000B 还要加 ICMP 头部 8B 所以进入 IP 层的 payload = 3000 + 8 = 3008B

## 抓包实验2：观察IPv6包

(1)

```

Type: IPv6 (0x86dd)
[Stream index: 0]
Internet Protocol Version 6, Src: 240c:c0a9:100d::3, Dst: 2402:f000:3
    0110 .... = Version: 6
    .... 0000 0000 .... .... .... .... .... = Traffic Class: 0x00 (DSCL)
    .... 1101 0100 0011 0111 1011 = Flow Label: 0xd437b
    Payload Length: 1456
    Next Header: Fragment Header for IPv6 (44)
    Hop Limit: 55
    ▶ Source Address: 240c:c0a9:100d::3
    ▶ Destination Address: 2402:f000:3:f001:fc68:9c16:c94f:2621
        [Stream index: 84]
    ▶ Fragment Header for IPv6
        ▶ [3 IPv6 Fragments (3008 bytes): #1074706(1448), #1074705(1448), #1074704(1448)]
    Internet Control Message Protocol v6

```

Version = 6

源地址 = 240c:c0a9:100d::3

目的地址 = 2402:f000:3:f001:fc68:9c16:c94f:2621

IPv6 地址长度 : 128 bit = 16 字节

(2)

IPv6 不允许路由器分片 · 只由源主机分片 通过 Fragment Extension Header ( 分片扩展头 · Next Header=44) 里面有 Identification / Fragment Offset / M 标志 若超 MTU · 路由器会回 ICMPv6 Packet Too Big 促使源端调整 (PMTUD)

(3)

```

.... .0. .... .... .... .... = LG bit: Globally unique address
.... .0. .... .... .... .... = IG bit: Individual address (unicast)
Type: IPv6 (0x86dd)
[Stream index: 0]
▼ Internet Protocol Version 6, Src: 240c:c0a9:100d::3, Dst: 2402:f000:3
  0110 .... = Version: 6
  ▶ .... 0000 0000 .... .... .... .... .... = Traffic Class: 0x00 (DSCP)
    .... 1101 0100 0011 0111 1011 = Flow Label: 0xd437b
    Payload Length: 1456
    Next Header: Fragment Header for IPv6 (44)
    Hop Limit: 55
  ▶ Source Address: 240c:c0a9:100d::3
  ▶ Destination Address: 2402:f000:3:f001:fc68:9c16:c94f:2621
    [Stream index: 84]
  ▼ Fragment Header for IPv6
    Next header: ICMPv6 (58)

```

IPv6 用 Hop Limit 替代 IPv4 的 TTL

简述题 (1) 什么情况下 IPv4 需要分段？哪里分段？哪里重组？

当 IPv4 报文长度 > 下一跳链路 MTU 且 DF=0 时需要分段。分段发生在：源主机或中间路由器 ( IPv4 允许路由器分片 ) 重组发生在：目的主机 ( 通常不在路由器重组 ) 。

(2) IPv6 头部不含 checksum · 如何做完整性校验？

IPv6 不做首部校验：依赖 链路层 CRC/FCS 检错；端到端依赖 传输层校验和 需要更强安全可用 IPsec 做认证/完整性保护。