实验二 ARP 与 ICMP

【实验目的】

1. 掌握 ARP 协议的报文格式
2. 掌握 ARP 协议的工作原理
3. 理解 ARP 高速缓存的作用
4. 掌握 ICMP 协议的报文格式
5. 理解不同类型 ICMP 报文的具体意义
6. 了解常见的网络故障

【实验学时】

建议 2 学时

【实验环境配置】

采用网络结构二

【实验原理】

ARP 协议

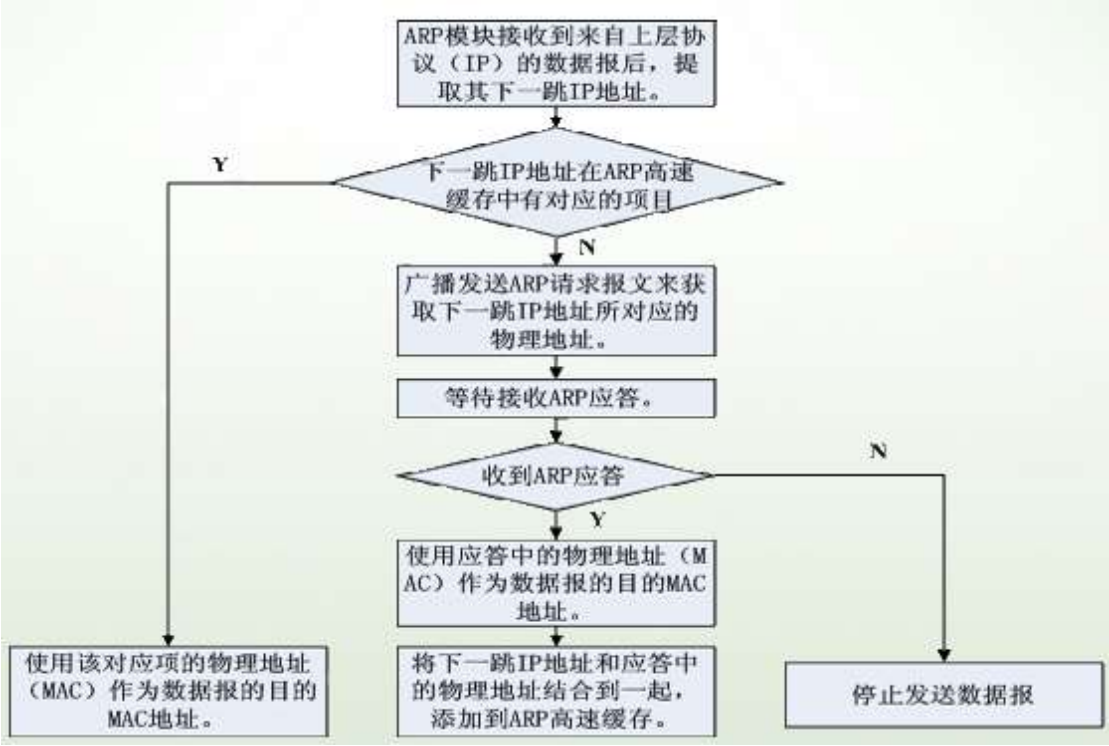
一、使用 IP 协议的以太网中 ARP 报文格式

<table>
<tr><td colspan="2">硬件类型（值为 1）</td><td>协议类型（值为 0800H）</td></tr>
<tr><td>硬件长度（值为 6）</td><td>协议长度（值为 4）</td><td>操作：请求 1，响应 2</td></tr>
<tr><td colspan="3">发送 MAC 地址（6 字节）</td></tr>
<tr><td colspan="3">发送 IP 地址（4 字节）</td></tr>
<tr><td colspan="3">目标端 MAC 地址（6 字节）（并未包含在请求报文中）</td></tr>
<tr><td colspan="3">目标端 IP 地址（4 字节）</td></tr>
</table>

字段说明：
硬件类型：表示硬件类型，例如：1 表示以太网。
协议类型：表示要映射的协议类型，例如 0x0800 表示 IP 地址。
硬件长度：指明硬件地址长度，单位是字节，MAC 是 48 位，长度是 6 个字节。
协议长度：高层协议地址的长度，对于 IP 地址，长度是 4 个字节。
操作字段：共有二种操作类型，1 表示 ARP 请求，2 表示 ARP 应答。
发送方 MAC：6 个字节的发送方 MAC 地址。

发送方 IP： 4 个字节的发送方 IP 地址。
目的 MAC：6 个字节的目的 MAC 地址。
目的 IP： 4 个字节的目的 IP 地址。

二、 ARP 地址解析过程



【实验步骤】

主机 B 启动静态路由服务（方法：在命令行方式下，输入“staticroute_config”）。按照拓扑结构图连接网络，使用拓扑验证检查连接的正确性。

拓扑验证截图：

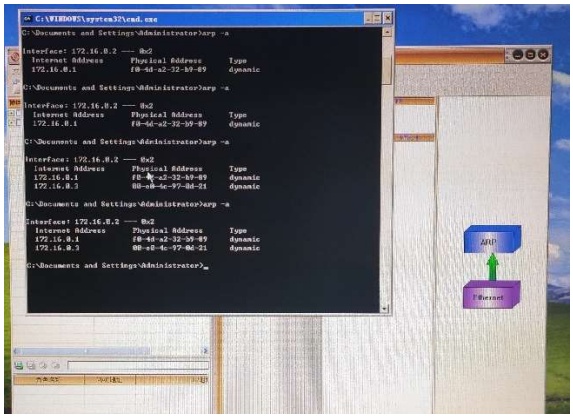
备注：在实际过程中，主机 A 无法通过拓扑验证，但主机 A 可以和各个其他地址相互通信。主机 A 配置的 IP 地址为 172.16.1.6，在此不保证接入主机 A 的拓扑验证图如图所示。

练习一：领略真实的 ARP（同一子网）

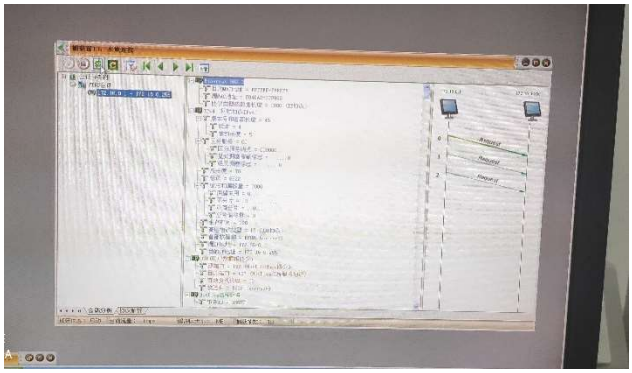
1. 主机 A、B、C、D、E、F 在命令行下运行“arp -a”命令，察看 ARP 高速缓存表，并回答以下问题：
    - ARP 高速缓存表由哪几项组成？

    ARP 告诉缓存由 Internet Address(IP 地址) Physical Address(MAC 地址) Type(static 静态分配 dynamic 动态)三项组成。

2. 主机 A、B、C、D 启动协议分析器，打开捕获窗口进行数据捕获并设置过滤条件（提取 ARP、ICMP）。
3. 主机 A、B、C、D 在命令行下运行“arp -d”命令，清空 ARP 高速缓存。
4. 主机 A ping 主机 D（172.16.1.4）。
5. 主机 A、B、C、D 停止捕获数据，并立即在命令行下运行“arp -a”命令察看 ARP 高速缓存。
    - 结合协议分析器上采集到的 ARP 报文和 ARP 高速缓存表中新增加的条目，简述 ARP 协议的报文交互过程以及 ARP 高速缓存表的更新过程。



如图所示为主机 E ping 主机 F 过程中 arp 告诉缓存的变化，在此过程中，arp 项目新增了 172.16.0.3 一条。当主机 E(172.16.0.2)ping 主机 F(172.16.0.3)时，先查找 arp 高速缓存是否有其对应的 MAC 地址，当发现没有时，主机 E 向本局域网广播 ARP 请求帧(对应的目的 MAC 地址为 FFFFFF-FFFFFF，IP 地址为 172.16.0.3)，当主机 B 接受到 ARP 请求帧后，发现 IP 地址不符合，将此帧丢弃。当主机 C 接受到 ARP 请求帧后，将主机 B 的 IP 地址和 MAC 地址计入 ARP 告诉缓存，并向主机 B 单播 ARP 响应帧。最后主机 B 后，将主机 C 的 IP 地址和 MAC 地址加入高速缓存，完成 ARP 高速缓存表的更新。

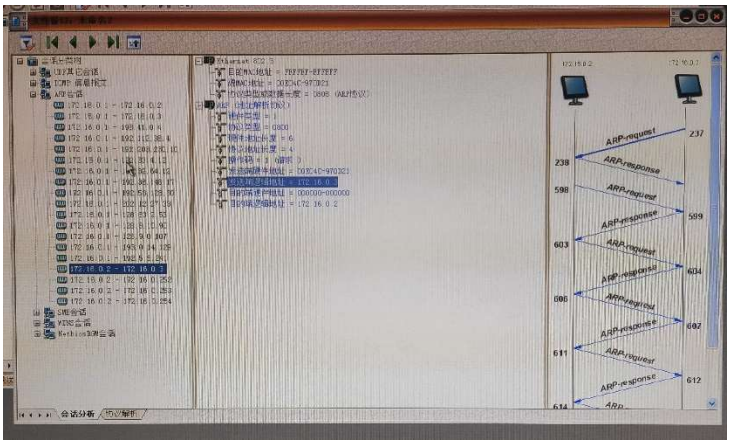


同时，我们应该注意到，此时主机 A，C，D 均没有收到 ARP 请求帧，说明 ARP 请求只能在一个局域网内广播，即符合不能扩域的特征。

练习二：编辑并发送 ARP 报文（同一子网）

1. 在主机 E 上启动仿真编辑器，并编辑一个 ARP 请求报文。其中:
   MAC 层： “目的 MAC 地址”设置为 FFFFFF-FFFFFF，
   “源 MAC 地址”设置为主机 E 的 MAC 地址。
   协议类型或数据长度：0806。
   ARP 层： “发送端 MAC 地址”设置为主机 E 的 MAC 地址，
   “发送端 IP 地址”设置为主机 E 的 IP 地址（172.16.0.2），
   “目的端 MAC 地址”设置为 000000-000000，
   “目的端 IP 地址”设置为主机 F 的 IP 地址（172.16.0.3）。
2. 主机 B、F 启动协议分析器，打开捕获窗口进行数据捕获并设置过滤条件（提取 ARP 协议）。
3. 主机 E、B、F 在命令行下运行“arp -d”命令，清空 ARP 高速缓存。
4. 主机 E 发送已编辑好的 ARP 报文。
5. 主机 E 立即在命令行下运行“arp -a”命令察看 ARP 高速缓存。
6. 主机 B、F 停止捕获数据，分析捕获到的数据，进一步体会 ARP 报文交互过程。

主机 B 截图

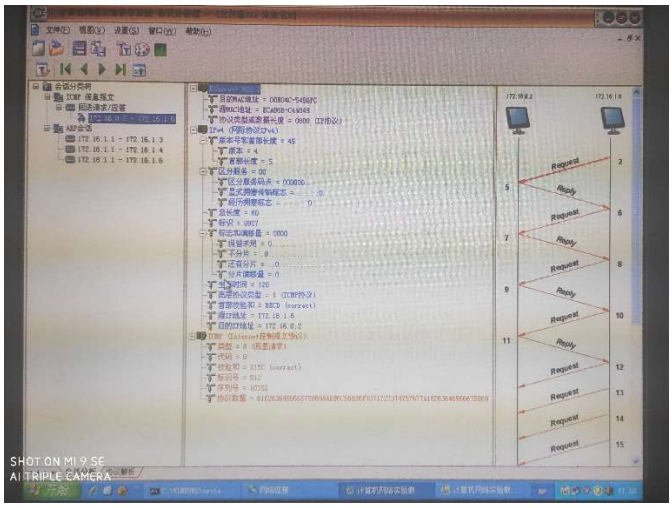


ARP 报文交互过程已在练习一中给出，故不再重复。

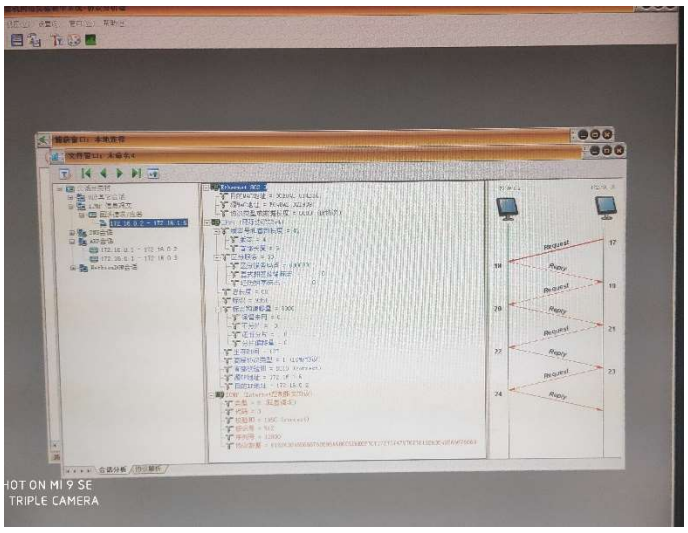
练习三：跨路由地址解析（不同子网）

1. 主机 A、B、C、D、E、F 在命令行下运行“arp -d”命令，清空 ARP 高速缓存。
2. 主机 A、B、C、D、E、F 重新启动协议分析器，打开捕获窗口进行数据捕获并设置过滤条件（提取 ARP、ICMP）。
3. 主机 A ping 主机 E（172.16.0.2）。
4. 主机 A、B、C、D、E、F 停止数据捕获，察看协议分析器中采集到的 ARP 报文，并回答以下问题：
    - 单一 ARP 请求报文是否能够跨越子网进行地址解析？为什么？
    - ARP 地址解析在跨越子网的通信中所起到的作用？

主机 A 截图



主机 E 截图



经过分析两张截图后，发现 ARP 请求并没有跨越子网进行地址解析。原因有二：其一为 ARP 请求是连接数据链路层和网际层之间的桥梁。跨越子网的通信由路由器来完成，

没有必要知道跨越子网的主机对应的 MAC 地址。其二，路由器在收到 ARP 请求后不会向另外的端口的传播，即组织了 ARP 的跨域请求。

但在跨越子网通信时，仍然需要 ARP 服务。因为主机在跨越子网通信时，根据默认网关来进行和路由器的交互（即仍需要借助路由器进行通信），即主机和路由器之间需要 ARP 请求。

【思考问题】

1. ARP 分组的长度是固定的吗？试加以解释。

ARP 请求的长度不是固定的，但一般为 20 个字节。主要原因是 ARP 需要根据数据链路层和网际层的地址标识方法做出长度的相应调整。

2. 试解释为什么 ARP 高速缓存每存入一个项目就要设置 10-20 分钟的超时计时器。这个时间设置得太大或太小会出现什么问题？

ARP 高速缓存存储的是 IP 地址到 MAC 地址的映射，在实际生活中，我们可能会变动网络的拓扑结构，从而需要动态更新 ARP 高速缓存。时间的设置主要考虑因素为实际情况的变化频率以及 ARP 高速缓存的性能消耗，时间设置得太大或太小都不好。

3. 至少举出两种不需要发送 ARP 请求分组的情况。

目标 IP 地址为本地环回地址或者目标 IP 到 MAC 地址的映射位于 ARP 高速缓存表中。

ICMP

【实验原理】

- 目的不可达报文

类型：3	代码：0 至 15	检验和
未使用（全 0）		
收到的 IP 数据报的一部分，包括 IP 首部以及数据报数据的前 8 个字节		

- 源端抑制报文

类型：4	代码：0	检验和
未使用（全 0）		
收到的 IP 数据报的一部分，包括 IP 首部以及数据报数据的前 8 个字节		

- 超时报文

类型：11	代码：0 或 1	检验和
未使用（全 0）		
收到的 IP 数据报的一部分，包括 IP 首部以及数据报数据的前 8 个字节		

- 参数问题

类型：12	代码：0 或 1	检验和
指针	未使用（全 0）	
收到的 IP 数据报的一部分，包括 IP 首部以及数据报数据的前 8 个字节		

- 改变路由

类型：5	代码：0 到 3	检验和
目标路由器 IP 地址		
收到的 IP 数据报的一部分，包括 IP 首部以及数据报数据的前 8 个字节		

- 回送请求和回答

类型：8 或 0	代码：0	检验和
标识符		序号
由请求报文发送；由回答报文重复		

- 时间戳请求和回答

类型：13 或 14	代码：0	检验和
标识符		序号
原始时间戳		
接收时间戳		
发送时间戳		

- 地址掩码请求和回答

类型：17 或 18	代码：0	检验和
标识符		序号
地址掩码		

- 路由询问和通告

类型：10	代码：0	检验和
标识符		序号

类型：9	代码：0	检验和
地址数	地址项目长度	寿命
路由器地址 1		

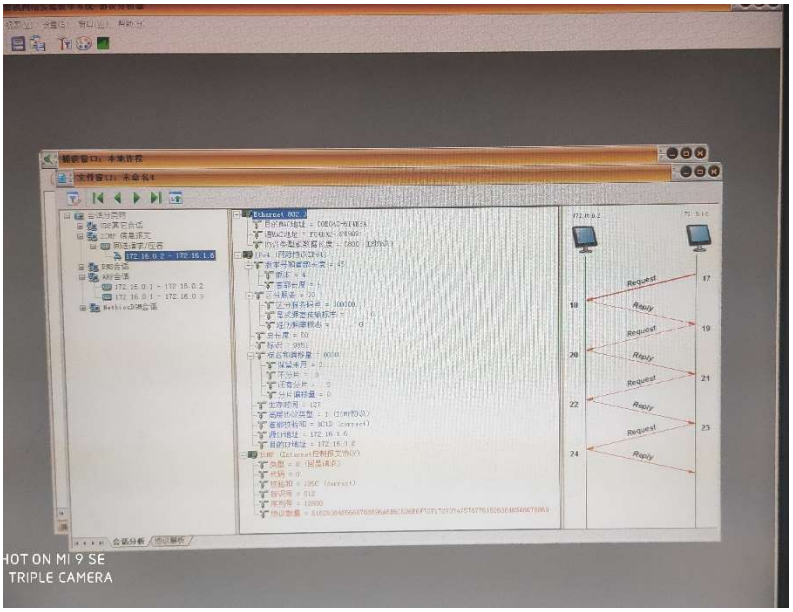
优先级 1
路由器地址 2
优先级 2
...

【实验步骤】

主机 B 启动静态路由服务（方法：在命令行方式下，输入“staticroute_config”）。 按照拓扑结构图连接网络，使用拓扑验证检查连接的正确性。

练习一：运行 Ping 命令

1. 主机 B、E、F 启动协议分析器，打开捕获窗口进行数据捕获并设置过滤条件（提取 ICMP 协议）。
2. 主机 A ping 主机 E（172.16.0.2）。
3. 主机 B、E、F 停止捕获数据，察看捕获到的数据，并回答以下问题：
   - 捕获的报文对应的“类型”和“代码”字段分别是什么？
   - 分析报文中的哪些字段保证了回送请求报文和回送应答报文的一一对应？



类型：6(回显)，代码：0

标识号和序列号两个字段保证了回送请求报文和回送应答报文一一对应。

练习二：ICMP 差错报文

1. 目的端不可达
   a. 主机 B、C、E、F 启动协议分析器捕获数据，并设置过滤条件（提取 ICMP）。
   b. 在主机 A 上 ping 172.16.2.10（不存在的 IP）。

c. 主机 B、C、E、F 停止捕获数据。察看捕获到的数据，并回答以下问题： 捕获到的是哪一种目的端不可达报文？

2. 超时

1. 在主机 D 上启动仿真编辑器，编写一个发送给主机 E（172.16.0.2）的 ICMP 数据帧。其中：

MAC 层：

目的 MAC 地址：主机 B 的 MAC 地址（对应于 172.16.1.1 接口的 MAC）。

源 MAC 地址：D 的 MAC 地址。

协议类型或数据长度：0800。

IP 层：

总长度：包含 IP 层和 ICMP 层长度。

TTL：0。

高层协议类型：1。

校验和：在其他字段填充完毕后，计算并填充。

源 IP 地址：D 的 IP 地址。

目的 IP 地址：E 的 IP 地址。

ICMP 层：

类型：8。

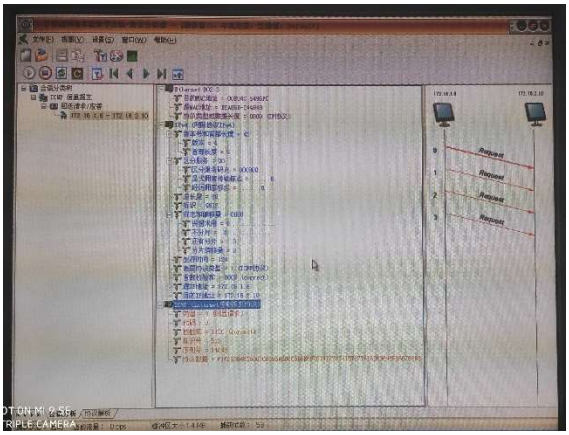
代码字段：0。

校验和：在 ICMP 其他字段填充完毕后，计算并填充。

其他字段使用默认值。

2. 主机 B、E、F 启动协议分析器捕获数据，并设置过滤条件（提取 ICMP 协议）。
3. 主机 D 发送已编辑好的数据帧。
4. 主机 B、E、F 停止捕获数据，察看并分析捕获到的数据。
5. 主机 B 在命令行方式下输入 recover_config 命令，停止静态路由服务。

目的端不可达



超时

【思考问题】

1. 为什么要限制由失效的 ICMP 差错报文再产生一个 ICMP 报文？

失效的 ICMP 差错报文的报告并不是必须的，其可以通过上层的重传来重现这个过程。且如果失效的 ICMP 差错报文再产生一个 ICMP 报文，可能造成无限次产生失效的 ICMP 差错报文，是不可取的。

2. 主机 A 向主机 B 发送数据报。主机 B 从未收到该数据报，而主机 A 也从未收到出问题的通知。试给出可能发生的情况的两种不同解释。

第一种情况是物理链路故障，即发送数据报后，其随即消失，没有任何差错报文产生。

第二种情况是主机 A 本生发生了故障，造成无法发出数据报，也无法收到出现问题的通知。或者主机 B 的 IP 地址被劫持，也可能是 host 配置文件的更改造成的。

3. 试用表说明，什么样的 ICMP 报文是由路由器发送出的，什么样的 ICMP 报文是由非目的主机发送出的，以及什么样的 ICMP 报文是由目的主机发送出的。

ICMP 报文类型	可能的发送者
目的不可达报文	目的主机/路由器/非目的主机(当使用管理时)
源端抑制报文	路由器
超时报文	路由器(TTL)，目的主机(分片没有全部到达)
参数问题	路由器(首部)，目的主机(可选项)
改变路由	路由器
回送请求和回答	目的主机
时间戳请求和回答	目的主机
地址掩码请求和回答	目的主机
地址询问和通告	目的主机