**网络实验二 地址解析协议（ARP）**

**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ARP请求和应答的实现方法

5. 掌握ARP缓存表的维护过程

**实验步骤**

**练习1：领略真实的ARP（同一子网）**

各主机打开协议分析器，进入相应的网络结构并验证网络拓扑的正确性，如果通过拓扑验证，关闭协议分析器继续进行实验，如果没有通过拓扑验证，请检查网络连接。本练习将主机A、B、C、D、E、F作为一组进行实验。

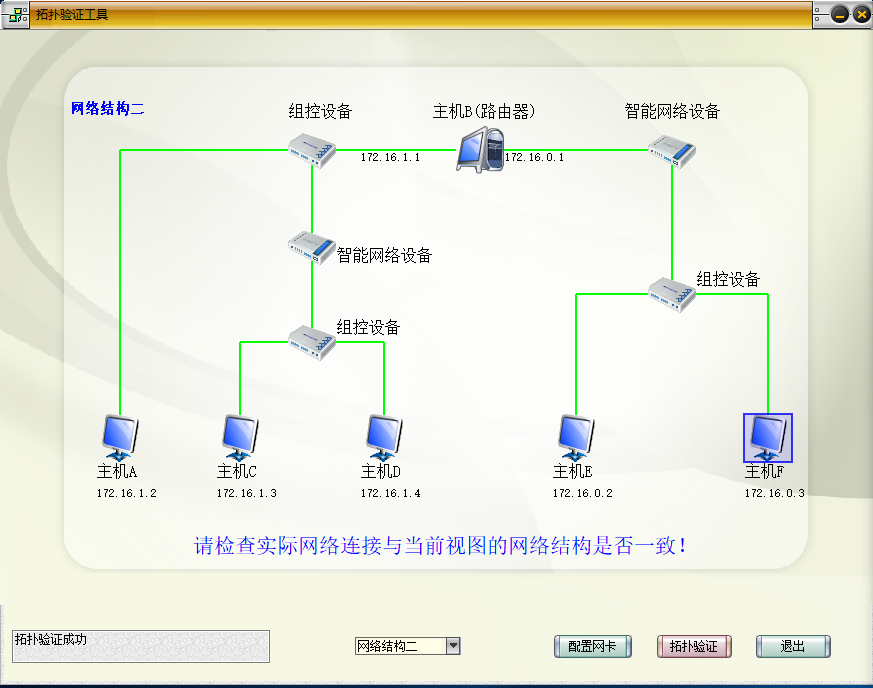
1. 主机A、B、C、D、E、F启动协议分析器，打开捕获窗口进行数据捕获并设置过滤条件（提取ARP、ICMP）。

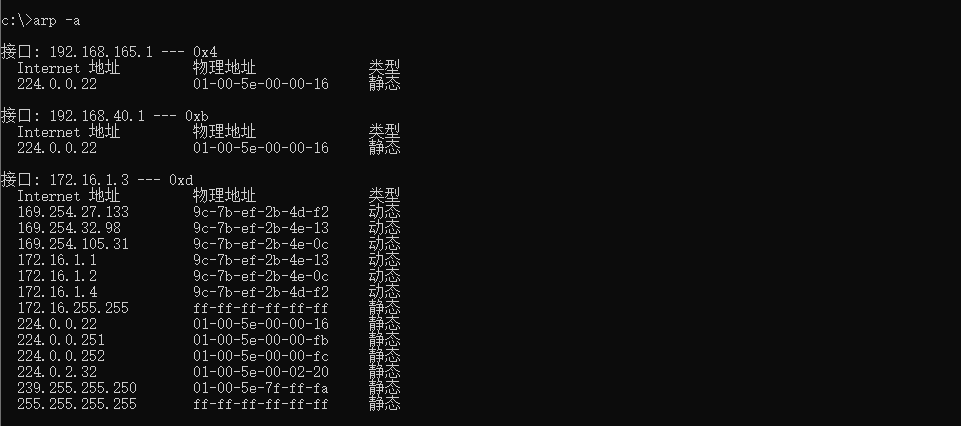
2. 主机A、B、C、D、E、F在命令行下运行“arp -d”命令，清空ARP高速缓存。

3. 主机A ping 主机D（172.16.1.4）。

4. 主机E ping 主机F（172.16.0.3）。

5. 主机A、B、C、D、E、F停止捕获数据，并立即在命令行下运行“arp -a”命令查看ARP高速缓存。





● ARP高速缓存表由哪几项组成？

答：（1）接口号：对应路由器的不同接口；（2）队列号：ARP使用不同的队列将等待地址解析的分组进行排队，发往同一个目的地的分组通常放在同一个队列中；（3）尝试：表示这个项目发送出了多少次的ARP请求（4）超时：表示一个项目以秒为单位的寿命；（5）硬件地址：目的硬件地址，应答返回前保持为空；（6）协议地址：目的高层协议地址如IP地址。

● 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。

答：以主机Aping主机D为例，当发送数据时，主机A会在自己的ARP缓存表中寻找是否有目标IP地址。如果找到了，也就知道了目标MAC地址，直接把目标MAC地址写入帧里面发送就可以了；如果在ARP缓存表中没有找到目标IP地址，主机A就会在网络上发送一个广播，这表示向同一网段内的所有主机发出这样的询问：“我是172.16.1.2,我的硬件地址是"0025B3-188783”，请问IP地址为172.16.1.4的MAC地址是什么？”网络上其他主机并不响应ARP询问，只有主机D接收到这个帧时，才向主机A做出这样的回应，这样，主机A就知道了主机D的MAC地址，它就可以向主机D发送信息了。同时A和D还同时都更新了自己的ARP缓存表(因为A在询问的时候把自己的IP和MAC地址一起告诉了D)，下次A再向主机D或者D向A发送信息时，直接从各自的ARP缓存表里查找就可以了。

**练习2：编辑并发送ARP报文（同一子网）**

本练习将主机A、B、C、D、E、F作为一组进行实验。

1. 在主机E上启动协议编辑器，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：

发送端硬件地址：设置为主机E的MAC地址

发送端逻辑地址：设置为主机E的IP地址（172.16.0.2）

目的端硬件地址：设置为000000-000000

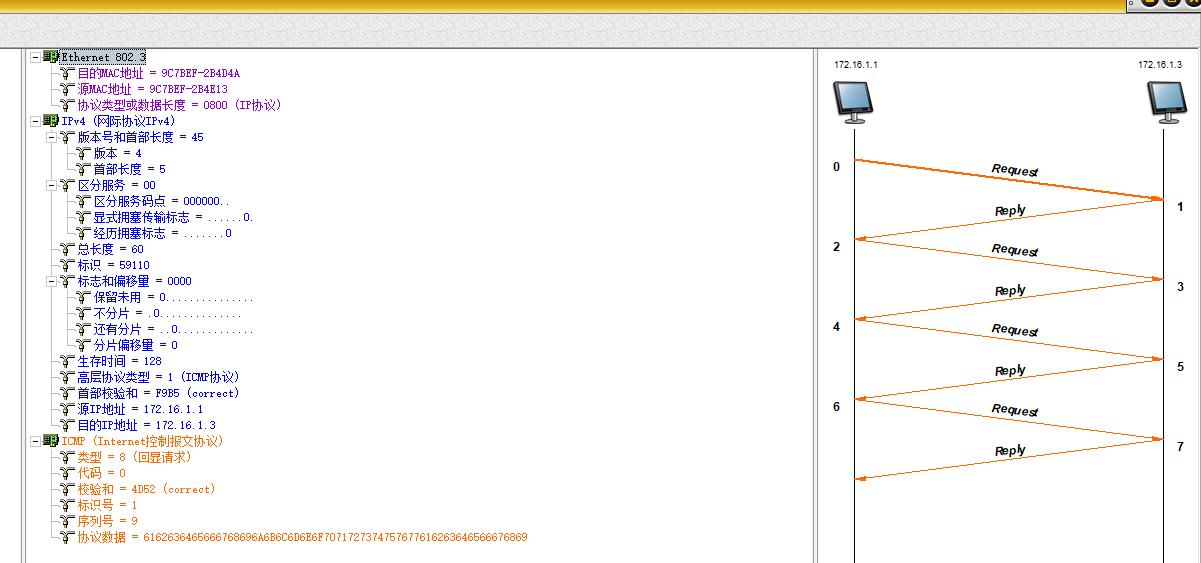
目的端逻辑地址：设置为主机F的IP地址（172.16.0.3）

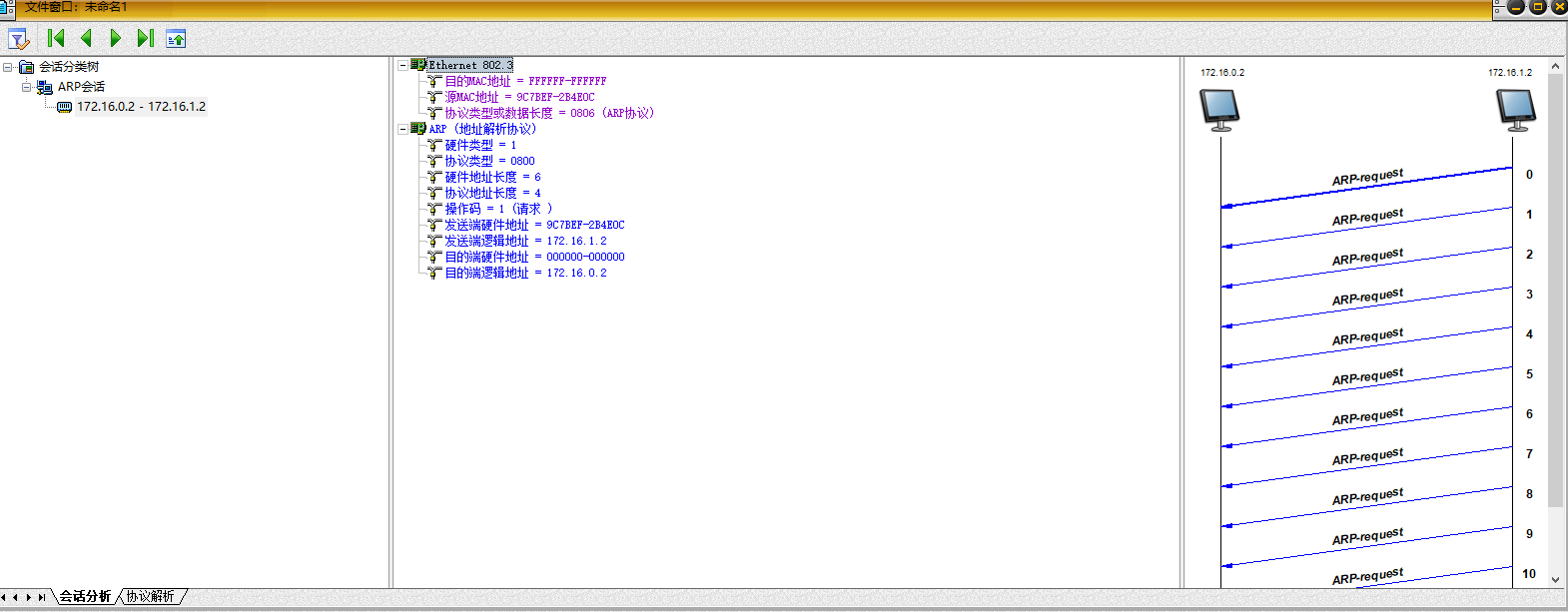
2. 主机B、F启动协议分析器，打开捕获窗口进行数据捕获并设置过滤条件（提取ARP协议）。

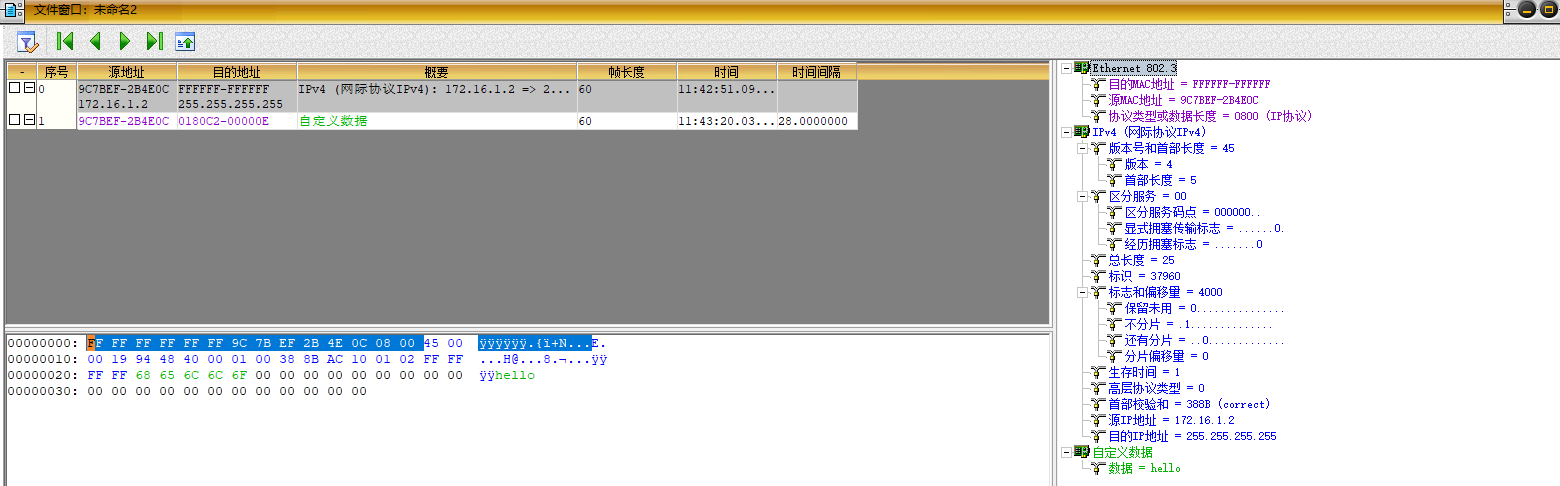
3. 主机B、E、F在命令行下运行“arp -d”命令，清空ARP高速缓存。主机E发送已编辑好的ARP报文。

4. 主机B、F停止捕获数据，分析捕获到的数据，记录ARP报文交互过程。

● 记录实验结果







**练习3：跨路由地址解析（不同子网）**

本练习将主机A、B、C、D、E、F作为一组进行实验。

1. 主机B在命令行方式下输入staticroute\_config命令，开启静态路由服务。

2. 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。

3. 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）。

4. 主机A ping 主机E（172.16.0.2）。

5. 主机A、B、C、D、E、F停止数据捕获，查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？

答：不可以，ARP报文的存活空间只限在子网中，因为ARP报文的请求是在网关下的数据请求，脱离子网ARP报文也就自动失效。

● ARP地址解析在跨越子网的通信中所起到的作用？

答：解析网关的MAC地址，ARP本身无法跨越不同网段。当数据要往外部网络时，通常是首先使用ARP请求网关路由器的MAC地址，之后将数据发往网关路由器，由网关路由器进行转发。

1. 主机B在命令行方式下输入recover\_config命令，停止静态路由服务。

