实验二：ARP 协议分析

一、实验目的

1、了解 ARP 协议；
2、熟悉 ARP 报文结构；
3、掌握 ARP 协议的工作原理。

二、实验学时

2 学时

扫码看步骤

三、实验类型

验证性

四、实验需求

1、硬件

每人配备计算机 1 台，不低于双核 CPU、8G 内存、500GB 硬盘。

2、软件

推荐 Ubuntu Desktop 操作系统，安装 GNS 3 仿真软件和 Wireshark 报文分析软件。
支持 Windows 操作系统，安装 GNS 3 仿真软件和 Wireshark 报文分析软件。

3、网络

计算机使用固定 IP 地址接入局域网，并支持对互联网的访问。

4、工具

无。

五、实验任务

1、完成 ARP 报文结构分析；
2、完成 VLAN 内 ARP 解析过程的分析；
3、完成 VLAN 间 ARP 解析过程的分析；
4、完成跨三层设备不同网络间 ARP 解析过程分析。

六、实验内容及步骤

在实验一的基础上开展本次实验，拓扑结构如图 2-1 所示。

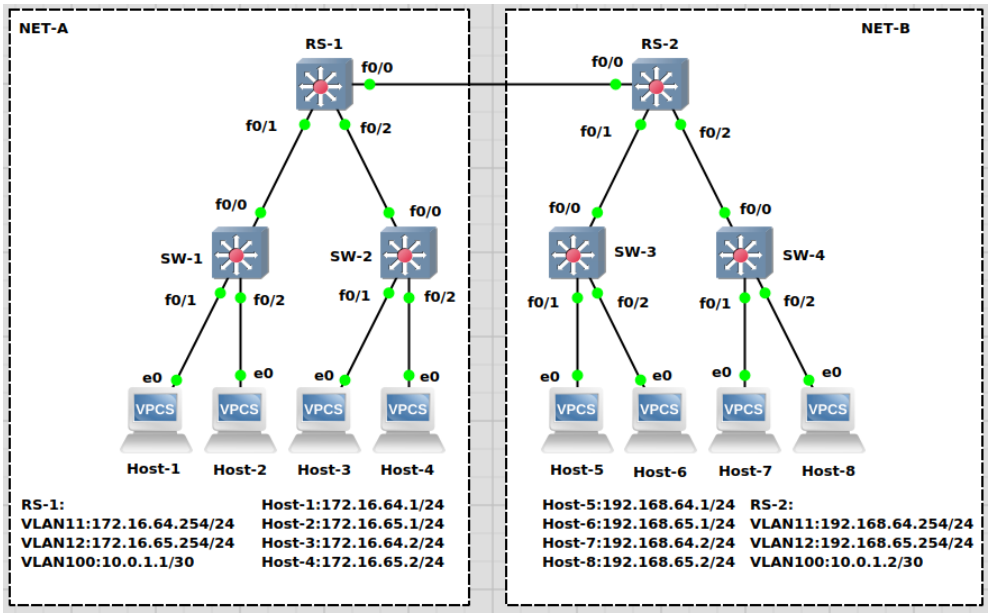

图 2-1 网络拓扑

任务 1：ARP 报文结构分析（15 分）

步骤 01：清空主机 Host-1 的 ARP 表

在 Host-1 终端上，通过命令清空 ARP 表。

参考命令：

```
clear arp
```

步骤 02：使用 Wireshark 记录主机 Host-1 的所有通信报文

右击 Host-1 与 SW-1 的链路，选择“start capture”进行抓包，结果如图 2-2 所示。

步骤 03：在主机 Host-1 上 Ping 主机 Host-3

在 Host-1 终端上，执行 Ping 命令。

参考命令：

```
ping 172.16.64.2
```

步骤 04：在 Wireshark 上筛选出 Host-1 的 ARP 报文

在 Wireshark 的过滤器中输入“arp”，查看 Host-1 收发的 ARP 报文，如图 2-3 所示。

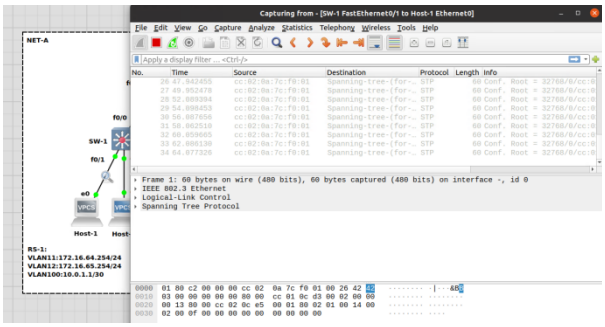

图 2-2 Wireshark 抓包

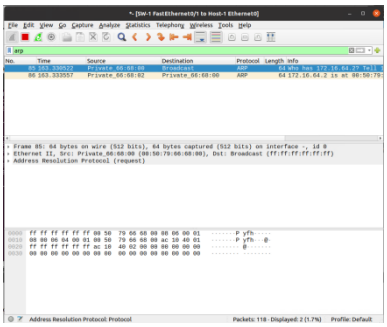

图 2-3 筛选 arp 报文

步骤 05：分析 Host-1 发出的 ARP 请求报文结构

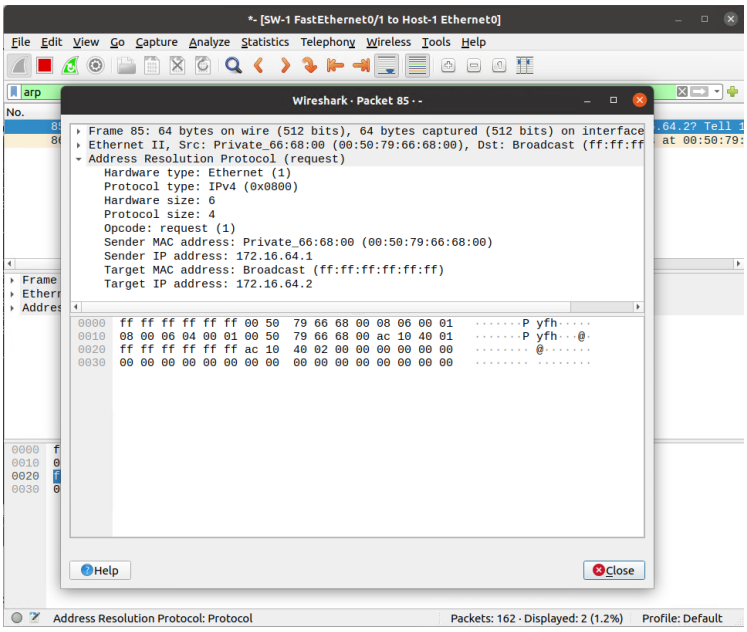

图 2-4 ARP 请求报文结构

在 Wireshark 中选择任意一条 ARP 请求报文进行详细分析，如图 2-4 所示，将分析结果填写到表 2-1。

表 2-1 ARP 请求报文分析

序号	字段名称	字段长度	起始位置	字段值	字段表示的信息
1	Hardware type		第　位		
2	Protocol type		第　位		
3	Hardware size		第　位		
4	Protocol size		第　位		
5	Opcode		第　位		
6	Sender MAC address		第　位		
7	Sender IP address		第　位		
8	Target MAC address		第　位		
9	Target IP address		第　位		

步骤 06：分析 Host-1 收到的 ARP 响应报文结构

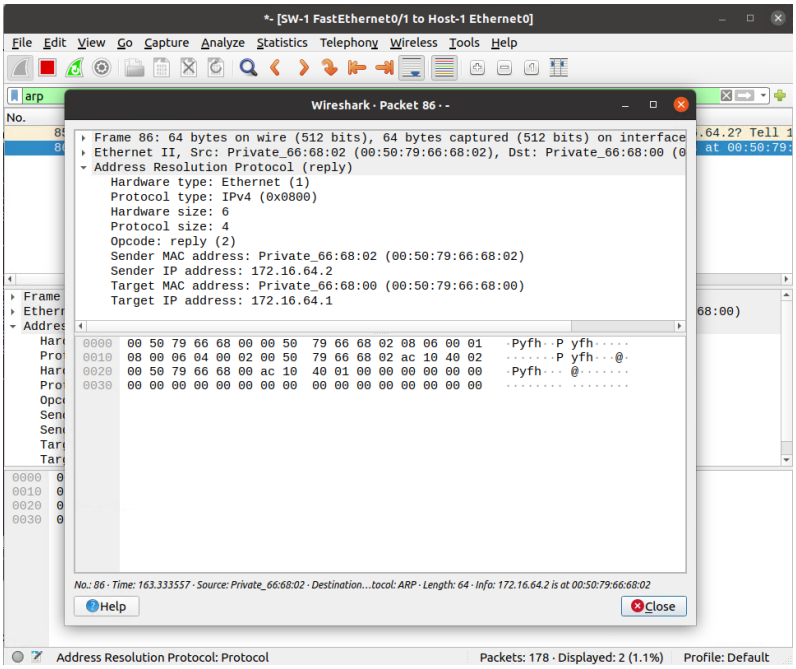

图 2-5 ARP 应答报文结构

在 Wireshark 中选择步骤 06 中请求报文对应的响应报文进行详细分析，如图 2-5 所示，分析结果填写到表 2-2。

表 2-2 ARP 应答报文分析

序号	字段名称	字段长度	起始位置	字段值	字段表示的信息
1	Hardware type		第 位		
2	Protocol type		第 位		
3	Hardware size		第 位		
4	Protocol size		第 位		
5	Opcode		第 位		
6	Sender MAC address		第 位		
7	Sender IP address		第 位		
8	Target MAC address		第 位		
9	Target IP address		第 位		

步骤 07：对比分析 ARP 请求报文和响应报文结构

比较 ARP 请求报文与响应报文的差别，并进行总结。

任务 2：VLAN 内 ARP 地址解析过程分析（15 分）

步骤 01：清空主机 Host-1 的 ARP 表。

步骤 02：使用 Wireshark 记录主机 Host-1 和 Host-3 之间所有链路的通信报文。

设置的抓取报文点共计 4 个，分别是主机 Host-1 至 SW-1、SW-1 至 RS-1、RS-1 至 SW-2、SW-2 至 Host-3 抓取报文，如图 2-6 所示。

步骤 03：在主机 Host-1 上 Ping 主机 Host-3。

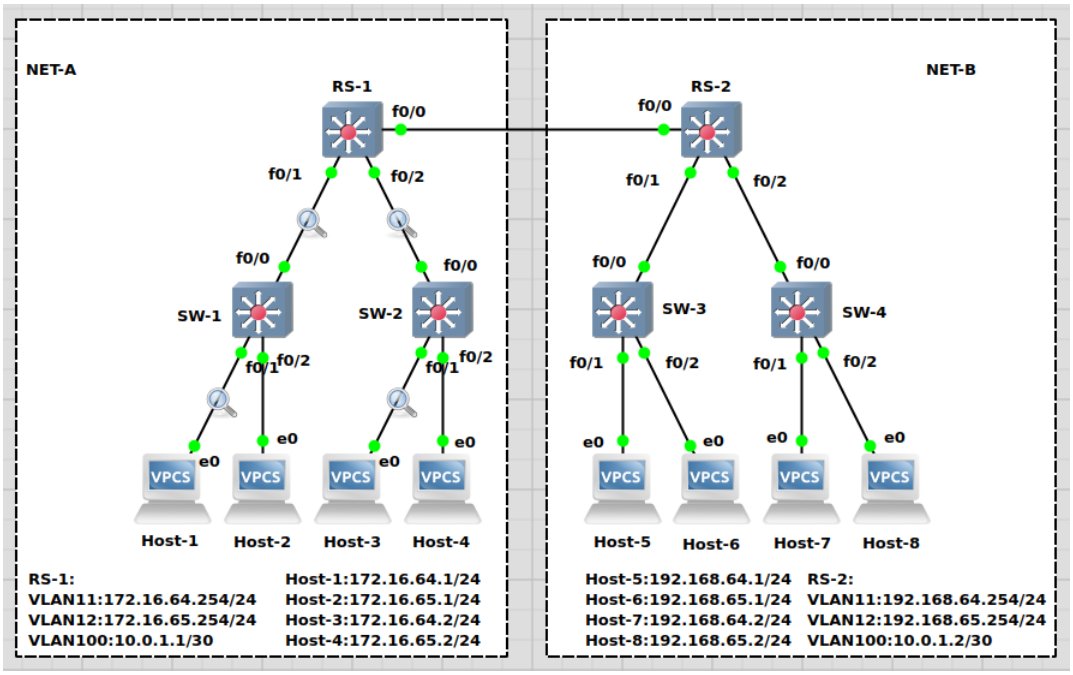

图 2-6 在 Host-1 和 Host-3 之间设置抓包点

步骤 04：在 Wireshark 上筛选出 Host-1 与 Host-3 通讯时的所有 ARP 报文。

提醒：

本任务的操作演示，参见教学视频。

教学视频地址：

https://internet.hactcm.edu.cn/mediaservice/network/syys/2023-2-2.mp4

Bilibili 访问地址：

https://www.bilibili.com/video/BV1NK4y1Y7J3?p=3

扫码看演示

步骤 05：分析主机 Host-1 在 Ping 主机 Host-3 时的 ARP 解析过程。

根据以上四个抓包点上获取的 ARP 数据，分析 ARP 解析过程，并填写表 2-3。

表 2-3 VLAN 内通信：Host-1 到 Host-3 间 ARP 解析过程分析

抓包点	报文字段	请求报文	响应报文
Host-1 至 SW-1	Sender MAC address		
	Sender IP address		
	Target MAC address		

	Target IP address		
SW-1 至 RS-1	**Sender MAC address**		
	Sender IP address		
	Target MAC address		
	Target IP address		
RS-1 至 SW-2	**Sender MAC address**		
	Sender IP address		
	Target MAC address		
	Target IP address		
SW-2 至 Host-2	**Sender MAC address**		
	Sender IP address		
	Target MAC address		
	Target IP address		

步骤 06：ARP 缓存的应用分析

当主机 Host-1 的 ARP 表中存在相关 ARP 记录时，Ping 主机 Host-3，是否会发送 ARP 请求？请通过实验进行验证。

任务 3： VLAN 间 ARP 地址解析过程分析（15 分）

步骤 01：清空主机 Host-1 的 ARP 表。

步骤 02：使用 Wireshark 记录主机 Host-1 和 Host-4 之间所有链路的通信报文。

设置的抓取报文点共计 4 个，分别是主机 Host-1 至 SW-1、SW-1 至 RS-1、RS-1 至 SW-2、SW-2 至 Host-4 抓取报文。

步骤 03：在主机 Host-1 上 Ping 主机 Host-4。

步骤 04：在 Wireshark 上筛选出 Host-1 与 Host-4 通讯时的所有 ARP 报文。

步骤 05：分析主机 Host-1 在 Ping 主机 Host-4 时的 ARP 解析过程。

根据以上四个抓包点上获取的 ARP 数据，分析 ARP 解析过程，并填写表 2-4。

表 2-4 VLAN 间通信：Host-1 到 Host-4 间 ARP 解析过程分析

抓包点	报文字段	请求报文	响应报文
Host-1 至 SW-1	**Sender MAC address**		
	Sender IP address		
	Target MAC address		
	Target IP address		
SW-1 至 RS-1	**Sender MAC address**		
	Sender IP address		
	Target MAC address		
	Target IP address		

RS-1 至 SW-2	Sender MAC address		
	Sender IP address		
	Target MAC address		
	Target IP address		
SW-2 至 Host-4	Sender MAC address		
	Sender IP address		
	Target MAC address		
	Target IP address		

步骤 06：ARP 解析过程总结

请根据表 2-1、表 2-2 的结果，分析总结在 ARP 解析过程，并对比分析 VLAN 内、VLAN 间通信时，ARP 解析过程的异同。

任务 4： 跨路由的 ARP 地址解析过程分析（15 分）

步骤 01：清空主机 Host-1 的 ARP 表。

步骤 02：使用 Wireshark 记录主机 Host-1 和 Host-8 之间所有链路的通信报文。

设置的抓取报文点共计 5 个，分别是主机 Host-1 至 SW-1、SW-1 至 RS-1、RS-1 至 RS-2、RS-2 至 SW-4、SW-4 至 Host-8 抓取报文，如图 2-7 所示。

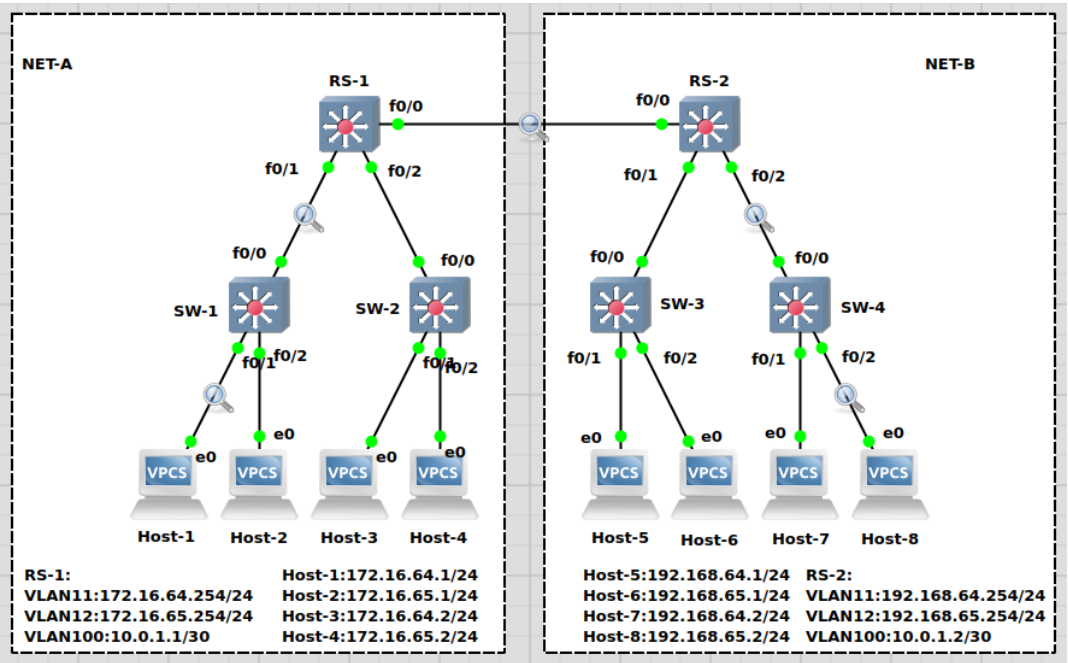

图 2-7 在 Host-1 和 Host-8 之间设置抓包点

步骤 03：在主机 Host-1 上 Ping 主机 Host-8。

步骤 04：在 Wireshark 上筛选出 Host-1 与 Host-8 通讯时的所有 ARP 报文。

步骤 05：分析主机 Host-1 在 Ping 主机 Host-8 时的 ARP 解析过程。

根据以上五个抓包点上获取的 ARP 数据，分析 ARP 解析过程，并填写表 2-5。

表 2-5 跨路有通信：Host-1 到 Host-8 间 ARP 解析过程分析

抓包点	报文字段	请求报文	响应报文
Host-1 至 SW-1	Sender MAC address		
	Sender IP address		
	Target MAC address		
	Target IP address		
SW-1 至 RS-1	Sender MAC address		
	Sender IP address		
	Target MAC address		
	Target IP address		
RS-1 至 RS-2	Sender MAC address		
	Sender IP address		
	Target MAC address		
	Target IP address		
RS-2 至 SW-4	Sender MAC address		
	Sender IP address		
	Target MAC address		
	Target IP address		
SW-4 至 Host-8	Sender MAC address		
	Sender IP address		
	Target MAC address		
	Target IP address		

注意：抓包点如有多条 ARP 请求或响应报文，请自行增加上述表格行数。

步骤 06：跨路由的 ARP 解析过程总结

请根据表 2-5 的结果，总结分析跨路由通信下的 ARP 解析过程。

七、实验考核

实验考核从【完成维度】和【时间维度】两个维度进行评分。

1、【完成维度】考核

本维度主要考核学生完成实验的程度以及对实验内容的理解程度，包括【任务完成度】【实验报告】和【回答问题】三个部分。具体如下：

（1）任务完成度（60 分）

学生在完成实验后，要当面提交教师检查实验结果。教师检查每个实验任务的完成情况，并根据实验指导书中每个任务的分值，给出任务完成度的分数。本项目满分 60 分。

（2）回答问题（40 分）

学生在完成实验后，要当面提交教师检查实验结果，并回答教师提问。教师根据学生回

答情况评分。本项目满分 40 分。

【注意】：教师提问时，可参考“八、思考与讨论”中的问题，从中随机选取 2-3 个问题进行提问。

2、【时间维度】考核

本维度主要考核学生完成实验的时间，具体如下：

（1）当堂提交（100 分起评）

本实验的实验课当堂提交并通过【完成维度】考核的，从 100 分起评。

（2）一周内提交（90 分起评）

本实验的实验课结束一周内提交并通过【完成维度】考核的，从 90 分起评，即本次实验考核最高 90 分。

（3）一周后提交（80 分起评）

本实验的实验课结束一周后提交并通过【完成维度】考核的，从 80 分起评，即本次实验考核最高 80 分。

（4）未提交（0 分）

本学期教学工作结束时，仍未提交的，本次实验考核 0 分。

八、思考与讨论

学生在做实验时，要结合实验内容和过程，讨论分析以下问题，以备教师提问

1. ARP 的英文名称是什么？中文名称是什么？该协议属于哪一层协议？在网络通信中，ARP 协议有什么作用？
2. 本实验中，进行报文分析的软件是什么？该软件的版本是什么？该软件有哪些主要功能？该软件的界面结构中包括哪些内容？
3. 本实验任务 1 中，步骤 01 是“清空主机 Host-1 的 ARP 表”，请自行查询资料，并结合实际操作，谈谈此处的“ARP 表”的作用是什么？该 ARP 表的内容是什么？为什么任务 1 要首先清空主机 Host-1 的 ARP 表？
4. 本实验任务 1 中，在 Host-1 和 SW-1 之间的链路上抓取一个 ARP 请求报文（注意，是请求报文，不是响应报文），将该报文展示给老师。问：该 ARP 请求报文是哪个设备发出的？它为什么要发出 ARP 请求报文？
5. 本实验任务 1 中，在 Host-1 和 SW-1 之间的链路上抓取一个 ARP 请求报文（注意，是请求报文，不是响应报文），将该报文展示给老师。问：该报文的首部中，包含哪些地址？分别是什么内容？
6. 本实验任务 1 中，在 Host-1 和 SW-1 之间的链路上抓取一个 ARP 请求报文（注意，是请求报文，不是响应报文），将该报文展示给老师。问：该报文的数据部分中，包含哪些字段（展示给老师）？其中的 Sender MAC address、Sender IP address、Target MAC address、Target IP address 四个字段分别表示什么意思？这四个字段的值分别是什么？

7. 本实验任务 1 中，在 Host-1 和 SW-1 之间的链路上抓取一个 ARP 请求报文（注意，是请求报文，不是响应报文），将该报文展示给老师。问：该报文的数据部分中，Target MAC address 字段的值是什么？为什么是这个值？Target IP address 字段的值是什么？在网络拓扑中，指出该 IP 地址所对应的设备。
8. 本实验任务 1 中，在执行步骤 03 时，问：Host-1 是否会发出 ARP 请求报文？为什么它会发出 ARP 请求报文？在实验指导书的图 2-1 所示的网络拓扑中，在哪些位置能抓取到 Host-1 发出的该 ARP 请求报文？请自行实验验证，并分析为什么在这些地方能抓取到 Host-1 发出的 ARP 请求报文？
9. 本实验任务 1 中，在执行步骤 03 时，分别在 Host-1 和 SW-1 之间、SW-1 和 RS-1 之间抓取 ARP 请求报文，分析：这两个地方抓取到 ARP 请求报文分别是谁发出的？对比分析这两个地方抓取的 ARP 请求报文的首部中的地址是什么？对比分析这两个地方抓取的 ARP 请求报文的数据部分中的 Sender MAC address、Sender IP address、Target MAC address、Target IP address 四个字段值分别是什么？
10. 本实验任务 1 中，在执行步骤 03 时，尝试在 SW-1 和 RS-1 之间抓取 ARP 响应报文。问：该响应报文是谁发出的？它为什么会发出该 ARP 响应报文？该响应报文首部中的地址是什么？该响应报文的数据部分中的 Sender MAC address、Sender IP address、Target MAC address、Target IP address 四个字段值分别是什么？
11. 本实验任务 1 中，对比分析 ARP 请求报文和响应报文的结构以及报文中各字段的值内容，谈谈有什么异同？
12. 本实验任务 2 中，步骤 05 中，对比分析实验指导书中所要求的四个抓包点上获取的 ARP 数据。问 1：对比分析在这四个抓包点上抓取的 ARP 请求报文中，Sender MAC address、Sender IP address、Target MAC address、Target IP address 四个字段的值，其结果如何？问 2：对比分析在这四个抓包点上抓取的 ARP 响应报文中，Sender MAC address、Sender IP address、Target MAC address、Target IP address 四个字段的值，其结果如何？
13. 本实验任务 3 中，步骤 05 中，对比分析实验指导书中所要求的四个抓包点上获取的 ARP 数据。问 1：对比分析在这四个抓包点上抓取的 ARP 请求报文中，Sender MAC address、Sender IP address、Target MAC address、Target IP address 四个字段的值，其结果如何？问 2：对比分析在这四个抓包点上抓取的 ARP 响应报文中，Sender MAC address、Sender IP address、Target MAC address、Target IP address 四个字段的值，其结果如何？
14. 本实验任务 3 中，步骤 05 中，所抓取到的 ARP 请求报文中，是否有 RS-1 发出的 ARP 请求报文？是否有 Host-4 发出的 ARP 请求报文？请自主通过实验去验证，若有，说明原因。若无，也请说明原因。

15. 本实验任务 4 中，在 RS-1 和 RS-2 之间，是否会抓到 ARP 请求报文？若能，说明该 ARP 请求报文是谁发出的？它为何会发出 ARP 请求报文？若不能，也说明原因。
16. 本实验任务 4 中，在 RS-2 和 SW-4 之间是否会抓到 ARP 请求报文？若有，谁发出的？它为什么会发出 ARP 请求报文？请先实验验证，然后根据实验结果进行分析。
17. 本实验任务 4 中，在 SW-4 和 Host-8 之间是否会抓到 ARP 请求报文？若有，谁发出的？它为什么会发出 ARP 请求报文？请先实验验证，然后根据实验结果进行分析。
18. 本实验任务 4 中，步骤 05 中，所抓取到的 ARP 请求报文中，是否有 Host-8 发出的 ARP 请求报文？请自主通过实验去验证，若有，说明原因。若无，也请说明原因。