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。

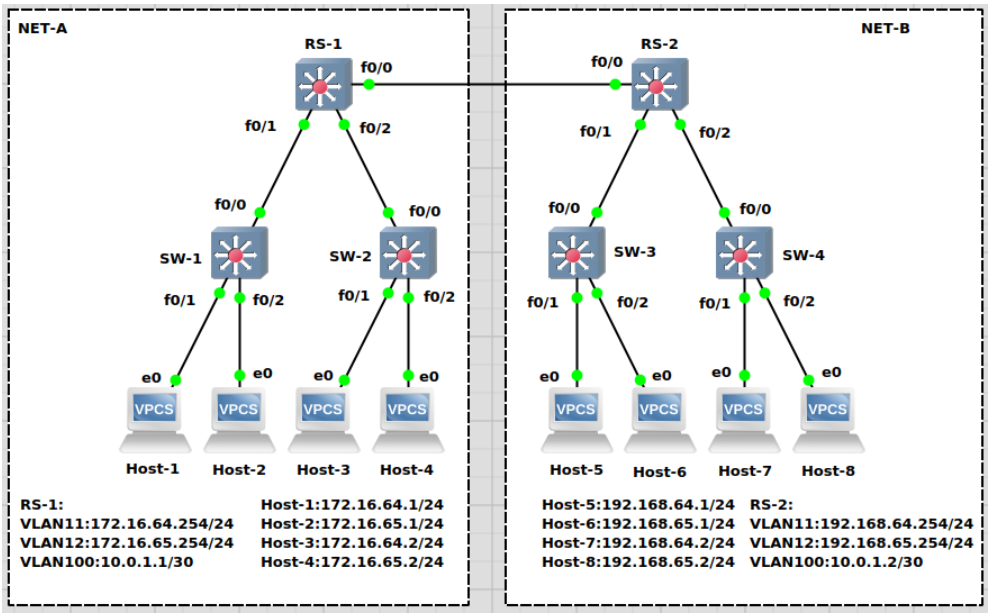

图 2-1 网络拓扑

任务 1：ARP 报文结构分析

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。

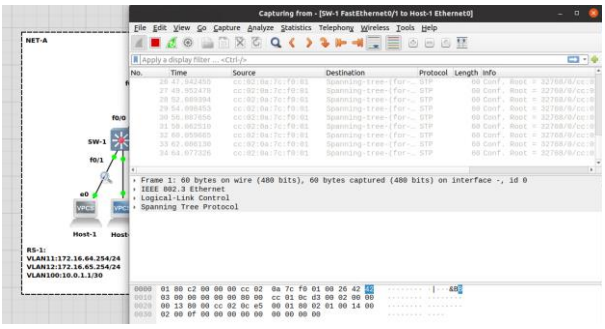

图 2-2 Wireshark 抓包

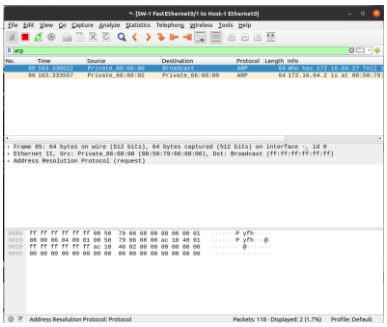

图 2-3 筛选 arp 报文

步骤 05：分析 Host-1 发出的 ARP 请求报文结构

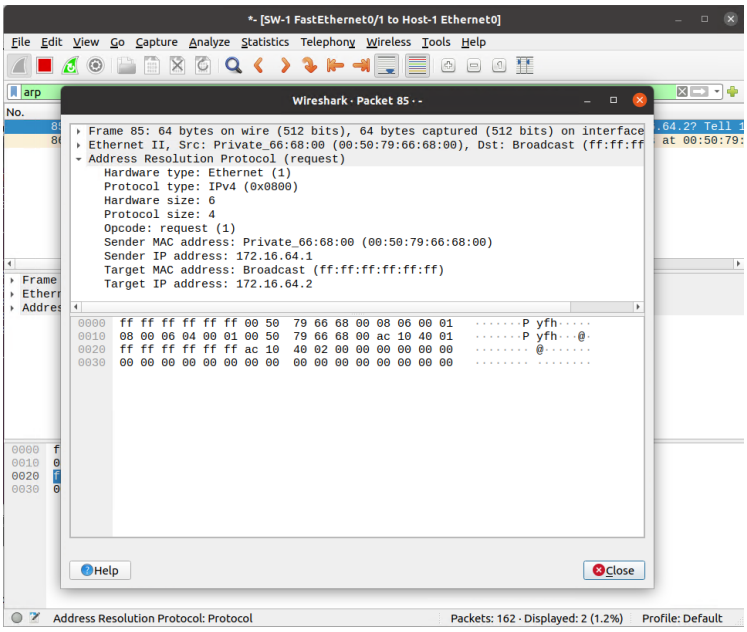

图 2-4 ARP 请求报文结构

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

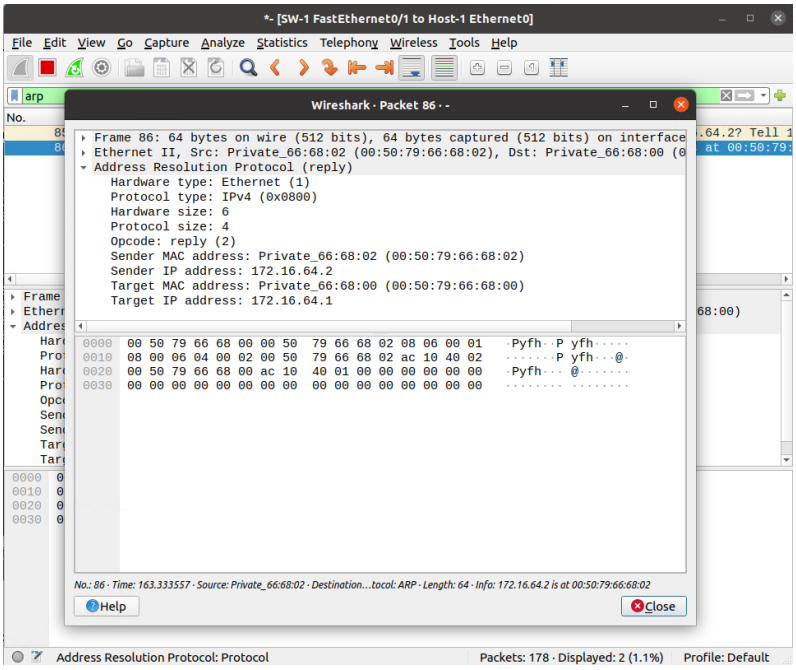

图 2-5 ARP 应答报文结构

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

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。

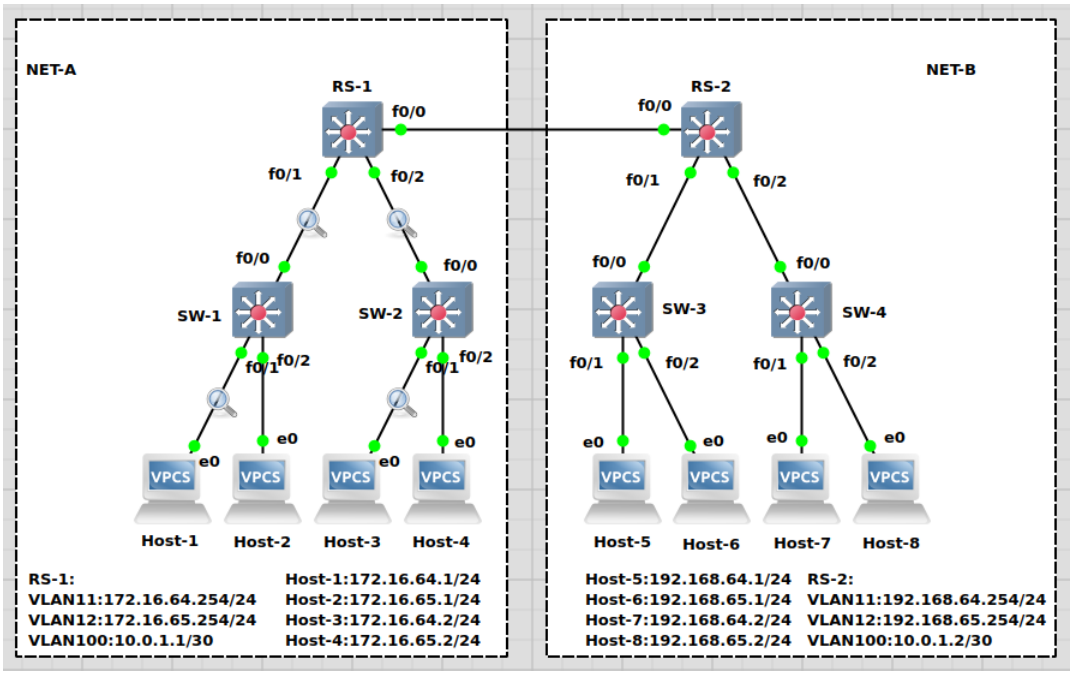

图 2-6 在 Host-1 和 Host-3 之间设置抓包点

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

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

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。

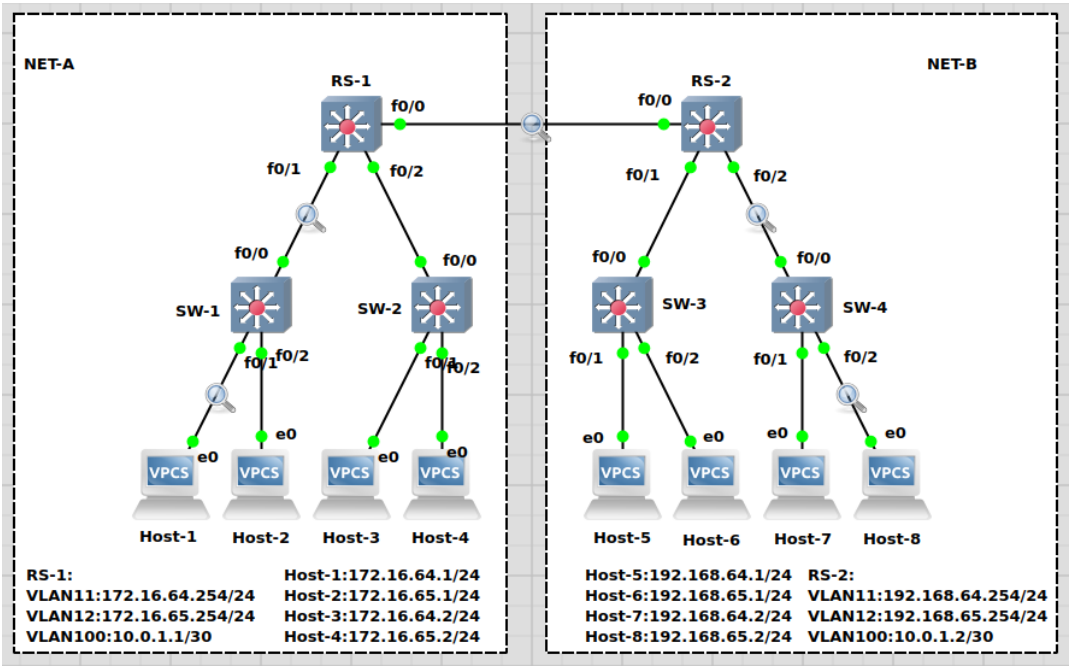

图 2-7 在 Host-1 和 Host-8 之间设置抓包点

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

1、任务说明

使用 GNS3 完成 ARP 协议的分析。

2、任务要求

要求 1：完成 ARP 报文结构分析；

要求 2：完成 VLAN 内 ARP 解析过程的分析；

要求 3：完成 VLAN 间 ARP 解析过程的分析；

要求 4：完成跨三层设备不同网络间 ARP 解析过程的分析。

3、考核要求

题目 1：完成表 2-1 的填写，并提交填写完的表格截图和对应的数据报文截图。
题目 2：完成表 2-2 的填写，并提交填写完的表格截图和对应的数据报文截图。
题目 3：完成表 2-3 的填写，并提交填写完的表格截图。
题目 4：请总结 VLAN 内 ARP 的通信过程。
题目 5：完成表 2-4 的填写，并提交填写完的表格截图。
题目 6：请总结 VLAN 间 ARP 的通信过程，并说明其和 VLAN 内 ARP 解析的不同。
题目 7：完成表 2-5 的填写，并提交填写完的表格截图。
题目 8：请总结跨路由的 ARP 解析过程。