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

扫码看演示

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。
支持 Windows 操作系统，安装 GNS 3 仿真软件。

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。

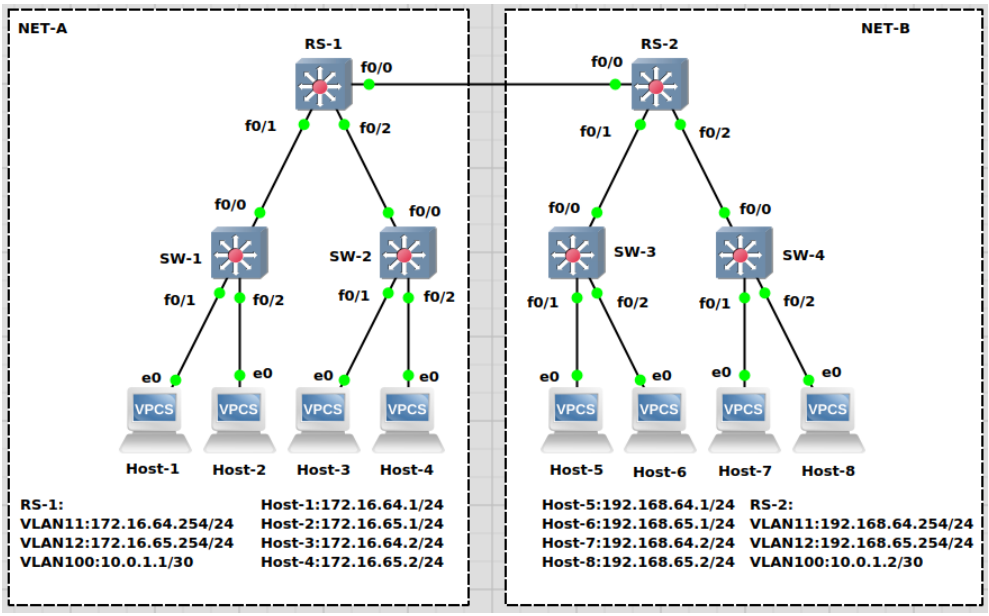

图 2-1 网络拓扑

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。

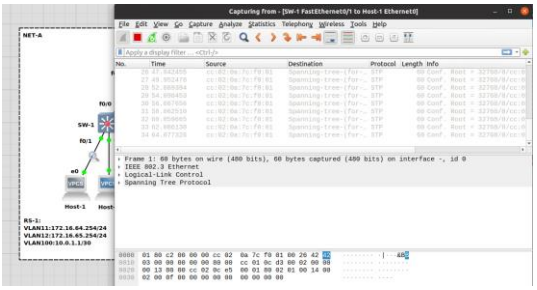

图 2-2 Wireshark 抓包

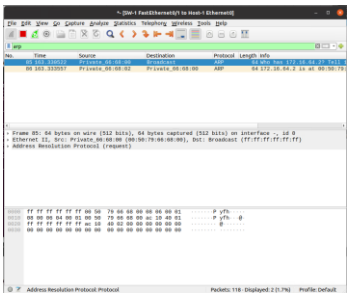

图 2-3 筛选 arp 报文

步骤 05：分析 Host-1 发出的 ARP 请求报文结构

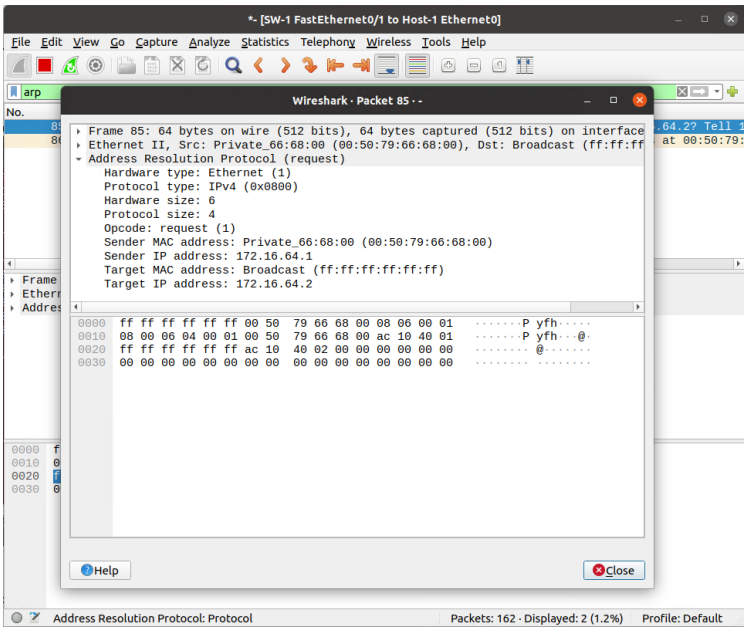

图 2-4 ARP 请求报文结构

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 1-1。

表 1-1 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		
10	数据包的详细内容				

步骤 07：分析 Host-1 收到的 ARP 响应报文结构

在 Wireshark 中选择任意一条响应报文进行详细分析，如图 2-5 所示，分析结果填写到

表 1-2。

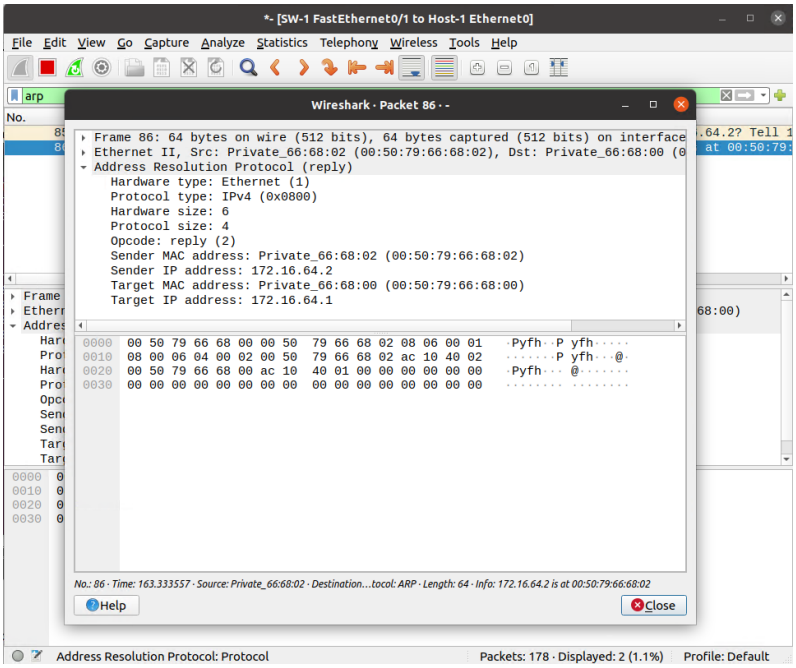

图 2-5 ARP 应答报文结构

表 1-2 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		
10	数据包的详细内容				

步骤 08：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 5 个关键差别，并填写表 1-3。

表 1-3 ARP 通信过程报文对比分析

序号	字段名称	请求报文		应答报文	
		字段值	字段表示信息	字段值	字段表示的信息
1					
2					
3					
4					
5					
6	详细对比描述				

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 的所有通信报文

分别在主机 Host-1 和 Host-3 抓取报文，如图 2-6 所示。

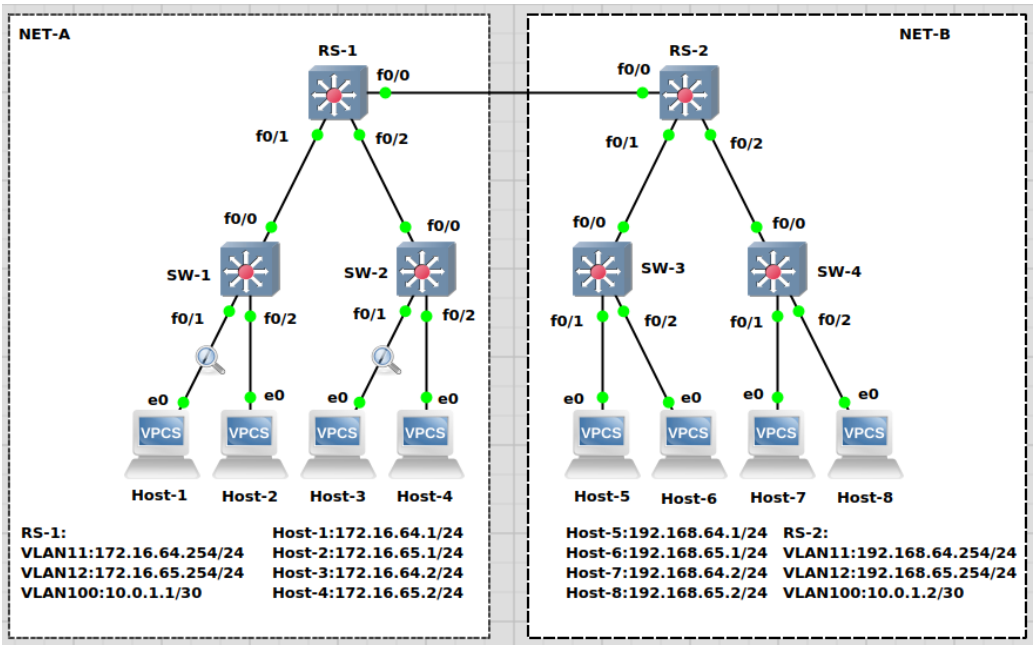

图 2-6 分别在 Host-1 和 Host-3 抓包

步骤 03：在主机 Host-1 上 Ping 主机 Host-3

步骤 04：在 Wireshark 上筛选出与 Host-3 对应的 ARP 请求与响应报文

在两个抓包点上筛选出 ARP 报文，如图 2-7 和 2-8 所示。

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

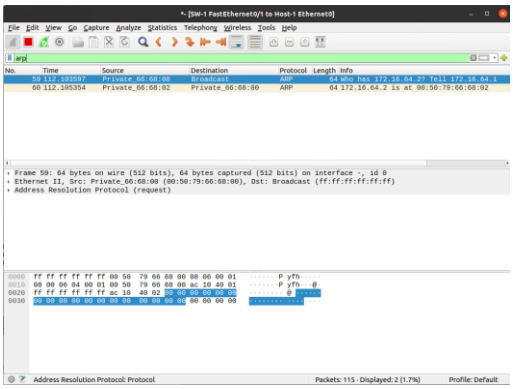

图 2-7 Host-1 收发的 ARP 报文

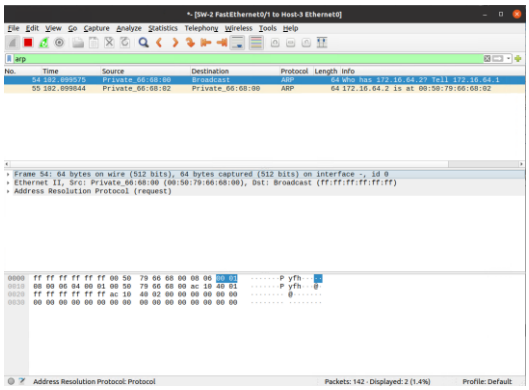

图 2-8 Host-3 收发的 ARP 报文

根据以上两个抓包点上获取的 ARP 数据，分析 ARP 地址解析过程，并填写表 2-1。

表 2-1 Host-1 到 Host-3 间 ARP 地址解析过程分析

Host-1	是否发送 ARP 请求报文	☐ 是	Target IP 地址	
	是否发送 ARP 应答报文	☐ 是	Target IP 地址	
	是否接收 ARP 请求报文	☐ 是	Sender IP 地址	
	是否接收 ARP 应答报文	☐ 是	Sender IP 地址	
Host-3	是否发送 ARP 请求报文	☐ 是	Target IP 地址	
	是否发送 ARP 应答报文	☐ 是	Target IP 地址	
	是否接收 ARP 请求报文	☐ 是	Sender IP 地址	
	是否接收 ARP 应答报文	☐ 是	Sender IP 地址	

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，再次 Ping 主机 Host-3，ARP 缓存表缓存的是 ARP 地址解析的结果。

当 ARP 缓存表中不存在相关 ARP 表项时，主机进行 ARP 地址解析，并将结果存入 ARP 缓存表，生成 ARP 表项。

当 ARP 缓存表中存在相关 ARP 表项，主机直接使用 ARP 表项中的 MAC 地址封装数据帧，不再进行 ARP 地址解析，如图 2-9 与 2-10 所示。

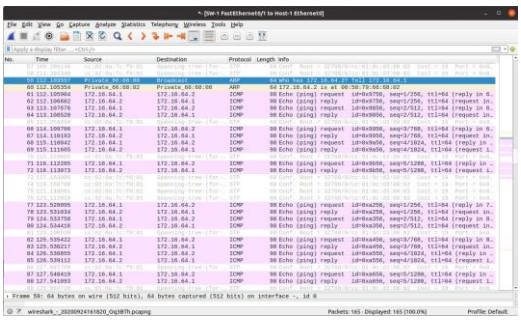

图 2-9 Host-1 收发的报文

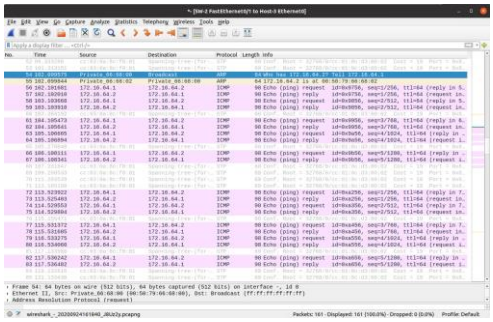

图 2-10 Host-3 收发的报文

步骤 07：对比分析 ARP 缓存对 ARP 地址解析的影响

根据以上两个抓包点的抓包，分析 ARP 表的作用，并填写表 2-2。

表 2-2 ARP 表对 ARP 地址解析的影响

分析项	是/否
不存在相关 ARP 表项时是否进行 ARP 地址解析	
存在相关 ARP 表项时是否进行 ARP 地址解析	

任务 3：不同 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 的所有通信报文

分别在主机 Host-1 和 Host-4 抓包，如图 2-11 所示。

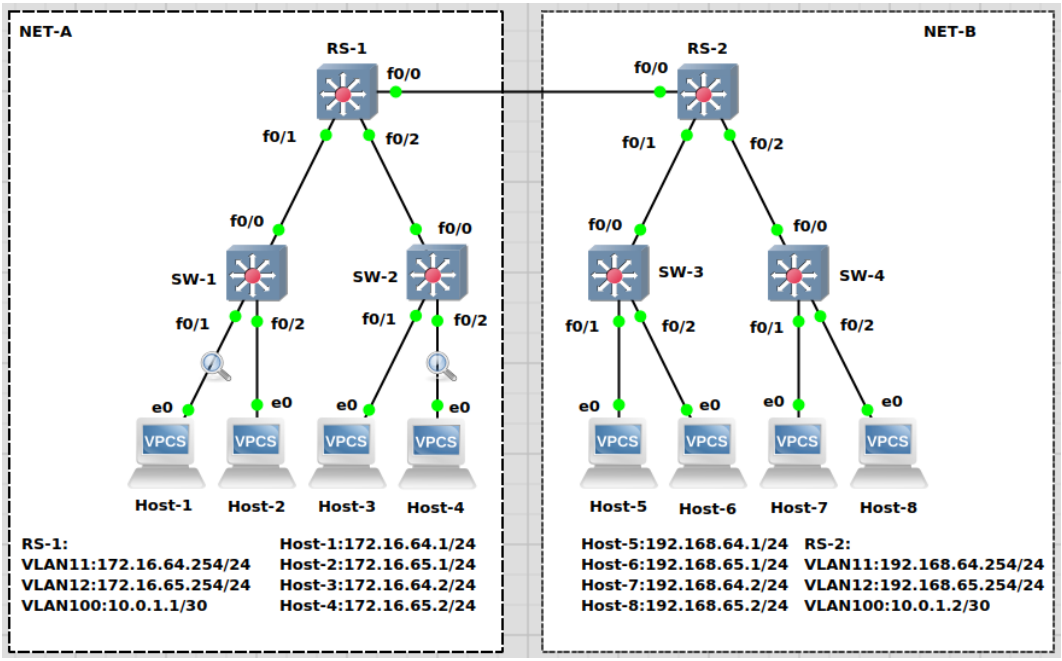

图 2-11 分别在 Host-1 和 Host-3 抓包

步骤 03：在主机 Host-1 上 Ping 主机 Host-4

步骤 04：在 Wireshark 上筛选出与 Host-4 对应的 ARP 请求与响应报文

在两个抓包点上筛选出的 ARP 报文如图 2-12 与 2-13 所示。

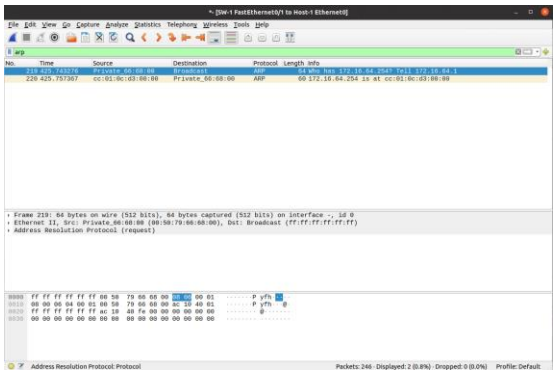

图 2-12 Host-1 收发的 ARP 报文

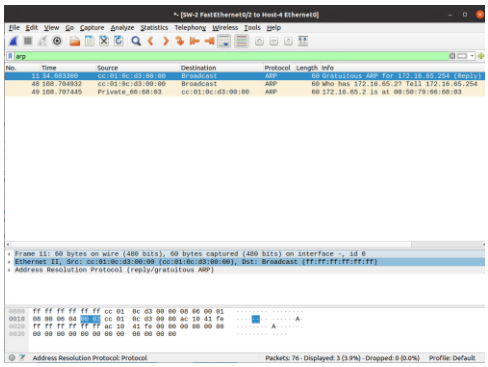

图 2-13 Host-4 收发的 ARP 报文

步骤 05：查看主机 Host-1 和三层交换机 RS-1 的路由表

主机 Host-1 和 RS1 的路由表如图 2-14、2-15 所示。

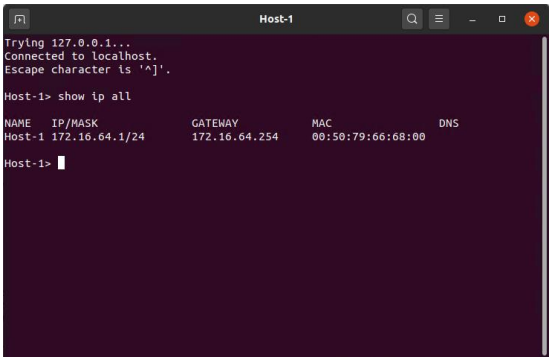

图 2-14 Host-1 路由表

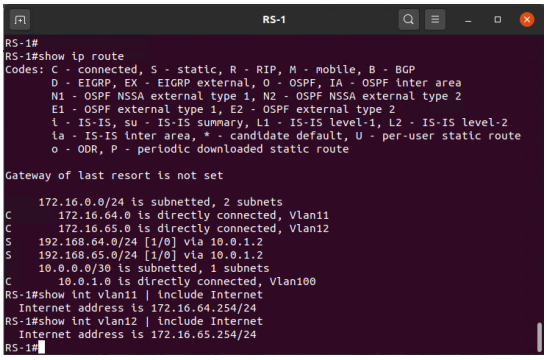

图 2-15 RS-1 路由表

步骤 06：分析主机 Host-1 在 Ping 主机 Host-4 时的 ARP 地址解析过程

根据以上两个抓包点的报文分析，分析 ARP 地址解析过程，并填写表 3-1。

表 3-1 Host-1 到 Host-4 间 ARP 地址解析过程分析

Host-1	是否发送 ARP 请求报文	☐ 是	Target IP 地址	
	是否发送 ARP 应答报文	☐ 是	Target IP 地址	
	是否接收 ARP 请求报文	☐ 是	Sender IP 地址	
	是否接收 ARP 应答报文	☐ 是	Sender IP 地址	
RS-1	是否发送 ARP 请求报文	☐ 是	Target IP 地址	
	是否发送 ARP 应答报文	☐ 是	Target IP 地址	
	是否接收 ARP 请求报文	☐ 是	Sender IP 地址	
	是否接收 ARP 应答报文	☐ 是	Sender IP 地址	

Host-4	是否发送 ARP 请求报文	□ 是	Target IP 地址	
	是否发送 ARP 应答报文	□ 是	Target IP 地址	
	是否接收 ARP 请求报文	□ 是	Sender IP 地址	
	是否接收 ARP 应答报文	□ 是	Sender IP 地址	

步骤 07：对比分析 Ping 主机 Host-3 与 Host-4 时 ARP 地址解析过程的不同

根据对以上两种情况的 ARP 地址解析的分析，比较地址解析过程中的不同之处，并填写表 3-2。

表 3-2 以上两种情况下 ARP 地址解析的不同之处

VLAN 内 ARP 地址解析过程	路由
	172.16.64.1->172.16.64.2
	对应 ARP 地址解析
	Sender:172.16.64.1->Target:172.16.64.2
VLAN 间 ARP 地址解析过程	路由
	172.16.64.1->172.16.64.254
	172.16.65.254->172.16.65.2
	对应 ARP 地址解析

任务 4：跨三层设备的网络间 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-8 的所有通信报文，记录三层交换机 RS-1 与 RS-2 之间的所有通信报文

分别在主机 Host-1 和 Host-8 以及 RS-1 与 RS-2 之间抓包，如图 2-16 所示。

步骤 03：在主机 Host-1 上 Ping 主机 Host-8

步骤 04：在 Wireshark 上筛选出与 Host-8 对应的 ARP 请求与响应报文

步骤 05：查看 RS-2 的路由表

三层交换机 RS-2 的路由表如图 2-17 所示。

步骤 06：分析主机 Host-1 在 Ping 主机 Host-8 时的 ARP 地址解析过程

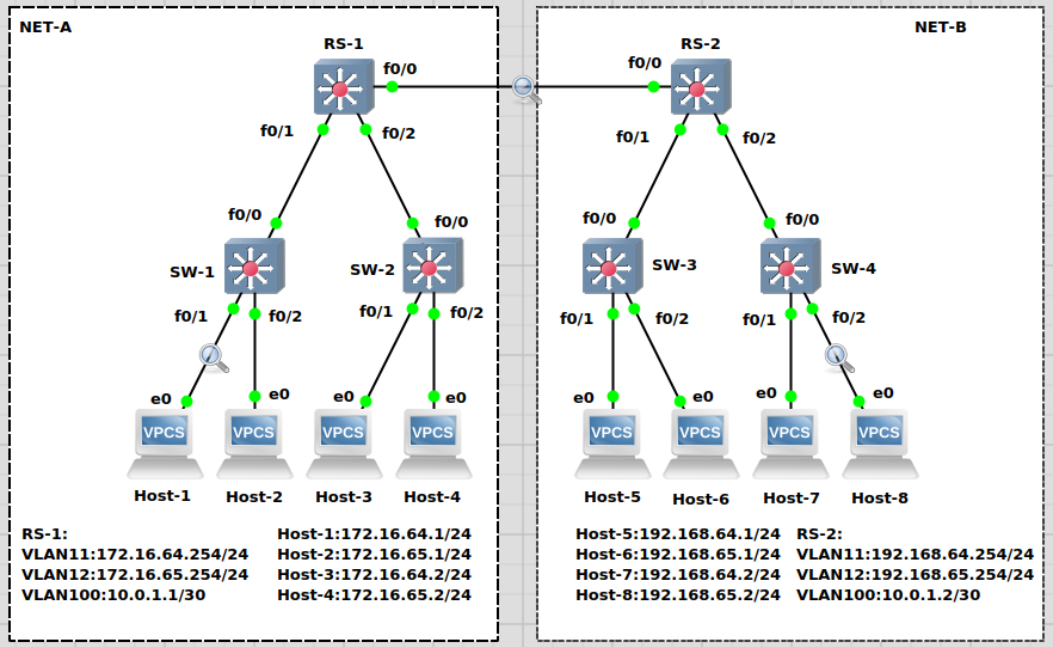

图 2-16 分别在 Host-1 和 Host-8 以及 RS-1 与 RS-2 之间抓包

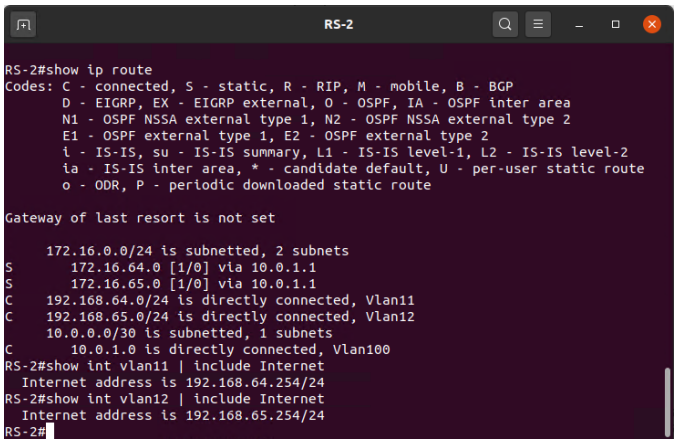

图 2-17 RS-2 路由表

根据以上三个抓包点报文数据，分析 ARP 地址解析过程，并填写表 4-1。

表 4-1 Host-1 到 Host-8 间 ARP 地址解析过程分析

Host-1	是否发送 ARP 请求报文	☐ 是	Target IP 地址	
	是否发送 ARP 应答报文	☐ 是	Target IP 地址	
	是否接收 ARP 请求报文	☐ 是	Sender IP 地址	
	是否接收 ARP 应答报文	☐ 是	Sender IP 地址	
RS-1	是否发送 ARP 请求报文	☐ 是	Target IP 地址	

	是否发送 ARP 应答报文	□ 是	Target IP 地址	
	是否接收 ARP 请求报文	□ 是	Sender IP 地址	
	是否接收 ARP 应答报文	□ 是	Sender IP 地址	
RS-2	是否发送 ARP 请求报文	□ 是	Target IP 地址	
	是否发送 ARP 应答报文	□ 是	Target IP 地址	
	是否接收 ARP 请求报文	□ 是	Sender IP 地址	
	是否接收 ARP 应答报文	□ 是	Sender IP 地址	
Host-8	是否发送 ARP 请求报文	□ 是	Target IP 地址	
	是否发送 ARP 应答报文	□ 是	Target IP 地址	
	是否接收 ARP 请求报文	□ 是	Sender IP 地址	
	是否接收 ARP 应答报文	□ 是	Sender IP 地址	

步骤 07：对比分析 Ping 主机 Host-3、Host-4 与 Host-8 时 ARP 地址解析过程的不同

根据对以上三种情况的 ARP 地址解析的分析，比较地址解析过程中的不同之处，并填写表 4-2。

表 4-2 以上三种情况下 ARP 地址解析的不同之处

VLAN 内 ARP 地址解析过程	路由
	对应 ARP 地址解析
VLAN 间 ARP 地址解析过程	路由
	对应 ARP 地址解析
跨三层设备不同网络间 ARP 地址解析过程	路由

	对应 ARP 地址解析

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：基于实验 1 的拓扑结构，在主机 Host-5 上 Ping 主机 Host-6，请提交【ARP 请求报文】与【ARP 响应报文】两张截图。

题目 2：分析【ARP 请求报文】，请填写以下信息。

字段“Protocol type”的字段长度_____，起始位置第_____位，字段值为_____，字段表示的信息为_____；

字段“Protocol size”的字段长度_____，起始位置第_____位，字段值为_____，字段表示的信息为_____；

字段“Opcode”的字段长度_____，起始位置第_____位，字段值为_____，字段表示的信息为_____。

题目 3：分析【ARP 响应报文】，请填写以下信息。

字段“Protocol type”的字段长度_____，起始位置第_____位，字段值为_____，字段表示的信息为_____；

字段“Protocol size”的字段长度_____，起始位置第_____位，字段值为_____，字段表示的信息为_____；

字段“Opcode”的字段长度_____，起始位置第_____位，字段值为_____，字段表示的信息为_____。

题目 4：请写出 ARP 请求报文与响应报文的 5 个关键差别。

题目 5：请写出跨三层设备的网络间 ARP 地址解析过程。