实验三：ICMP 协议分析

一、实验目的

1、了解 ICMP 报文结构和类型；
2、熟悉 ICMP 协议的作用；
3、掌握 PING 和 TRACEROUTE 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，安装 Wireshark 抓包工具。
支持 Windows 操作系统，安装 GNS 3 仿真软件，安装 Wireshark 抓包工具。

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 ICMP 报文结构的分析；
2、完成 ICMP 报文类型的分析；
3、完成 PING 通信分析；
4、完成 TRACEROUTE 通信分析。

六、实验内容及步骤

任务 1：分析 ICMP 报文结构（10 分）

（1）获取 ICMP 报文

在 Ubuntu 上启动 Wireshark 进行抓包，如图 3-1 所示，以 www.baidu.com 为目标主机，在终端上执行 PING 命令，要求 PING 通至少 4 次。

参考命令：

```
//因为 Wireshark 抓包需要 root 权限，所以通过以下命令启动
sudo wireshark
//在 Ubuntu Desktop 的终端中进行 Ping 操作
ping www.baidu.com
```

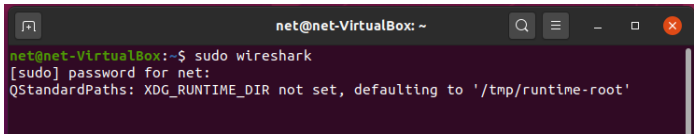

图 3-1 在终端启动 Wireshark

（2）查看 ICMP 报文结构

在 Wireshark 中停止截获报文，过滤出【ping www.baidu.com】产生的 ICMP 报文，查看 ICMP 报文结构。如图 3-2 所示。

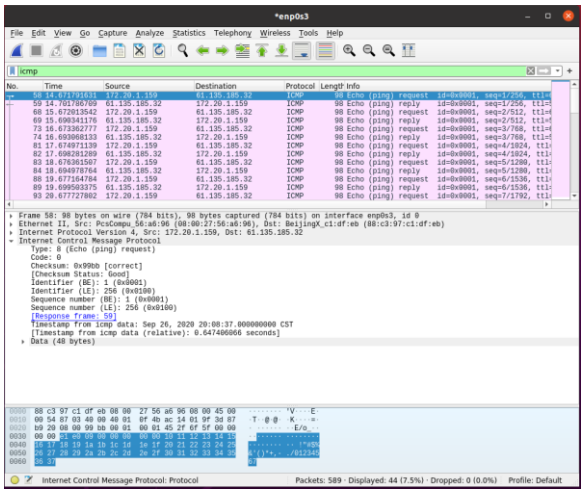

图 3-2 ICMP 报文

（3）分析 ICMP 报文结构

分析 ICMP 报文内容，填写表 3-1。

表 3-1 ICMP 报文结构分析

字段	大小（以字节为单位）	含义
Type		
Code		
Checksum		
Identifier		
Sequence		

任务 2：基于 PING 分析 ICMP 响应结果（20 分）

（1）使用主机 Host-8 对 NET-A 网络进行通信测试

在 GNS3 中打开实验一完成的网络仿真项目并开启所有设备，确保网络可以正常访问。在主机 Host-8 与交换机 SW-4 之间设置抓包点，如图 3-3 所示，启动 Wireshark 抓包。

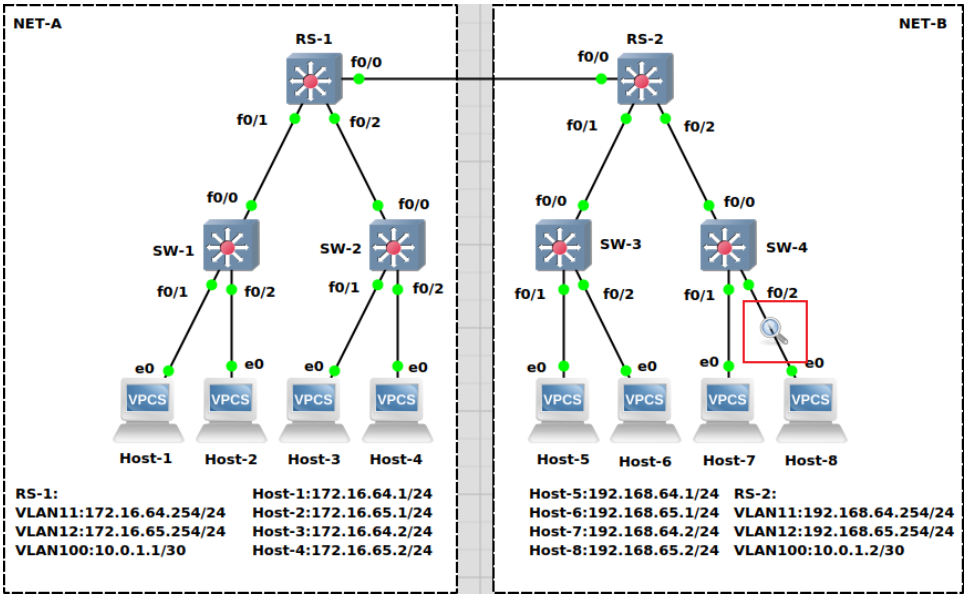

图 3-3 设置抓包点

（2）在主机 Host-1 运行正常的情况下，使用主机 Host-8 Ping 主机 Host-1。查看并分析主机 Host-8 和 Host-1 之间的 ICMP 报文，将结果填写入表 3-2 中。

表 3-2 ICMP 回显请求和回显应答报文信息

Host-8 Ping Host-1						
请求报文	源主机 IP	目的主机 IP	type	code	Identifier	Sequence
	请求内容（data）：					
响应报文	源主机 IP	目的主机 IP	type	code	Identifier	Sequence
	响应内容（data）：					

（3）在主机 Host-2 关机的情况下，使用主机 Host-8 Ping 主机 Host-2。查看并分析主机 Host-8 和 Host-2 之间的 ICMP 报文，将结果填写入表 3-3 中。

表 3-3 ICMP 回显请求和回显应答报文信息

Host-8 Ping Host-2						
请求报文	源主机 IP	目的主机 IP	type	code	Identifier	Sequence
	请求内容（data）：					
响应报文	源主机 IP	目的主机 IP	type	code	Identifier	Sequence
	响应内容（data）：					

（4）在主机 Host-3 网关配置错误的情况下，使用主机 Host-8 Ping 主机 Host-3。

查看并分析主机 Host-8 和 Host-3 之间的 ICMP 报文，将结果填写入表 3-4 中。

注意：请将 Host-3 的网关配置为同一网段内不存在的 IP 地址，例如 172.16.64.200。

表 3-4 ICMP 回显请求和回显应答报文信息

Host-8 Ping Host-3						
请求报文	源主机 IP	目的主机 IP	type	code	Identifier	Sequence
	请求内容（data）：					
响应报文	源主机 IP	目的主机 IP	type	code	Identifier	Sequence
	响应内容（data）：					

（5）使用主机 Host-8 Ping Net-A 部分中可配置未使用的任一 IP 地址。

查看并分析主机 Host-8 和可配置未使用的任一 IP 地址之间的 ICMP 报文，将结果填写入表 3-5 中。

注意：本步骤 Ping 的对象为 Net-A 部分可用但未配置的 IP 地址，例如 172.16.64.100。

表 3-5 ICMP 回显请求和回显应答报文信息

Host-8 Ping 172.16.64.100						
请求报文	源主机 IP	目的主机 IP	type	code	Identifier	Sequence
	请求内容（data）：					
响应报文	源主机 IP	目的主机 IP	type	code	Identifier	Sequence
	响应内容（data）：					

（6）使用主机 Host-8 Ping 不属于 Net-A 或 Net-B 的任一 IP 地址。

查看并分析主机 Host-8 和不属于 Net-A 或 Net-B 的任一 IP 地址（例如 172.16.0.100）之间的 ICMP 报文，将结果填写入表 3-6 中。

表 3-6 ICMP 回显请求和回显应答报文信息

Host-8 Ping 172.16.0.100						
请求报文	源主机 IP	目的主机 IP	type	code	Identifier	Sequence
	请求内容（data）：					
响应报文	源主机 IP	目的主机 IP	type	code	Identifier	Sequence
	响应内容（data）：					

任务 3：基于 TRACEROUTE 分析 ICMP 通信过程（30 分）

（1）设置抓包点，启动 Wireshark 进行抓包

在园区网中设置五个抓包点，如图 3-4 所示，启动 Wireshark 抓包。

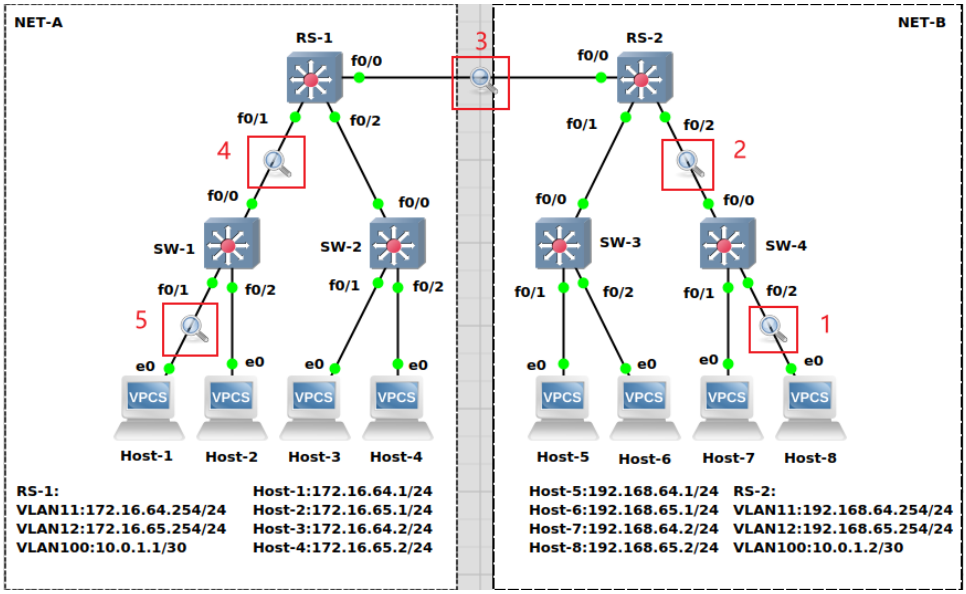

图 3-4 设置抓包点

（2）使用主机 Host-8 对主机 Host-1 进行 Traceroute 路由测试

在园区网中使用主机 Host-8 对主机 Host-1 进行 Traceroute 路由测试，由于在 GNS3 的 VPCS 中 trace 命令默认使用 UDP 协议，本实验步骤需要改变参数来实现使用 ICMP 协议进行通信，如图 3-5 所示。

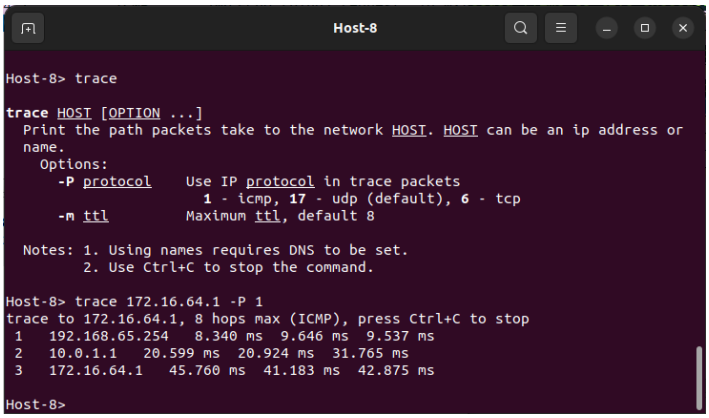

图 3-5 Traceroute 路由测试

参考命令：

```
//使用 ICMP 协议进行 Traceroute 路由测试
Host-8> trace 172.16.64.1 –P 1
```

（3）对抓包点 1 的 ICMP 报文进行分析

正常状态下，在抓包点 1 会记录 3 类共 18 条 ICMP 报文，其中 9 条请求报文、9 条响应报文。请按照报文相似度分类进行报文分析并填写表 3-7。

表 3-7 抓包点 1 的报文分析结果

报文 相似类	源 IP 地址	目的 IP 地址	TTL	Type	Code	报文内容描述或说明
第 1 类 共 6 条						
第 2 类 共 6 条						
第 3 类 共 6 条						

（4）对抓包点 2 的 ICMP 报文进行分析

正常状态下，在抓包点 2 会记录 3 类共 18 条 ICMP 报文，其中 9 条请求报文、9 条响应报文。请按照报文相似度分类进行报文分析并填写表 3-8。

表 3-8 抓包点 2 的报文分析结果

报文 相似类	源 IP 地址	目的 IP 地址	TTL	Type	Code	报文内容描述或说明
第 1 类 共 6 条						
第 2 类 共 6 条						
第 3 类 共 6 条						

（5）对抓包点 3 的 ICMP 报文进行分析

正常状态下，在抓包点 3 会记录 2 类共 12 条 ICMP 报文，其中 6 条请求报文、6 条响应报文。请按照报文相似度分类进行报文分析并填写表 3-9。

表 3-9 抓包点 3 的报文分析结果

报文 相似类	源 IP 地址	目的 IP 地址	TTL	Type	Code	报文内容描述或说明
第 1 类 共 6 条						
第 2 类						

共 6 条						

（6）对抓包点 4 的 ICMP 报文进行分析

正常状态下，在抓包点 4 会记录 1 类共 6 条 ICMP 报文，其中 3 条请求报文、3 条响应报文。请按照报文相似度分类进行报文分析并填写表 3-10。

表 3-10 抓包点 4 的报文分析结果

报文 相似类	源 IP 地址	目的 IP 地址	TTL	Type	Code	报文内容描述或说明
第 1 类 共 6 条						

（7）对抓包点 5 的 ICMP 报文进行分析

正常状态下，在抓包点 5 会记录 1 类共 6 条 ICMP 报文，其中 3 条请求报文、3 条响应报文。请按照报文相似度分类进行报文分析并填写表 3-11。

表 3-11 抓包点 5 的报文分析结果

报文 相似类	源 IP 地址	目的 IP 地址	TTL	Type	Code	报文内容描述或说明
第 1 类 共 6 条						

（8）分析相邻抓包点间的报文异同，并分析 Traceroute 工作原理

对五个抓包点得到的 ICMP 报文进行对比分析，分析相邻抓包点报文异同，说明 Traceroute 的工作原理。

分析思路建议：

- Traceroute 使用 ICMP 协议的工作原理。
- 主机 Host-8 为什么能够获取到路由器接口地址？为什么获取不到交换机的地址？
- 抓包点 1 和抓包点 2 的报文为什么相同？抓包点 4 和抓包点 5 的报文为什么相同？
- 同一抓包点的 ICMP 报文的源 IP 地址和目的 IP 地址是否相同？为什么？

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. ICMP 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，ICMP 协议有什么作用？
2. ICMP 报文的类型分为哪两类？从每一类 ICMP 报文中，各举出一个报文类型的例子，说明其作用，以及该类型的值。
3. 本实验任务 1 中，对于所抓取到的 ICMP 报文，查看其中一条 ICMP 报文的结构，问：其报文结构中的 Type 字段的值是多少？表示什么含义？除了这个值以外，Type 字段还有哪些值？举出 3 个例子，分别说明这些值的含义。
4. 本实验任务 1 中，对于所抓取到的 ICMP 报文，查看其中一条 ICMP 报文的结构，问：其报文结构中的 Code、Checksum、Identifier、Sequence 字段的值分别是什么？分别表示什么含义？
5. 本实验任务 2 的步骤 2 中，在网络通信正常，各主机运行正常的情况下，执行 Host-8 Ping Host-1：
   a) 所抓到 ICMP 回显请求报文中，首部里的源 IP 地址和目的 IP 地址分别是什么？源 MAC 地址和目的 MAC 地址又是什么？该报文的 type 字段值是多少？
   b) 所抓到的 ICMP 回显应答报文中，首部里的源 IP 地址和目的 IP 地址分别是什么？源 MAC 地址和目的 MAC 地址又是什么？该报文的 type 字段值是多少？
6. 本实验任务 2 的步骤 2 中，在网络通信正常，各主机运行正常的情况下，执行 Host-8 Ping Host-1。通过在 Host-8 到 Host-1 的路径中，每两个设备之间设置抓包点（例如 SW-

4 和 RS-2 之间、RS-2 和 RS-1 之间等），针对在每个抓包点所抓取到的 Host-8 发往 Host-1 的 ICMP 回显请求报文，分析每个报文中的 VLAN 标记，是否有 VLAN 标记？若无，说明原因。若有，说明 VID 值。

7. 本实验任务 2 的步骤 3 中，在网络通信正常，关闭 Host-2，其他主机运行正常的情况下，执行 Host-8 Ping Host-2：
   a) 执行该 Ping 命令后，屏幕上所显示的信息，与任务 2 的步骤 2 中执行完 Ping 命令所显示的信息有何不同？为什么会显示这样的信息？
   b) 对比该步骤中所抓取的 ICMP 报文和步骤 2 中所抓取的 ICMP 报文，有何不同？为什么出现这种区别？
   c) 在步骤 3 中，从 Host-8 发出的 ICMP 请求报文，是否到达了 Host-2？若到达了，尝试分析该报文的通信过程；若没有到达，说明在哪里被丢弃了？为什么被丢弃？（提醒：可结合 ARP 协议的应用进行分析）
8. 本实验任务 2 的步骤 4 中，在网络设备配置正常，Host-3 网关配置错误，其他主机运行正常的情况下，执行 Host-8 Ping Host-3：
   a) 执行该 Ping 命令后，屏幕上所显示的信息，与任务 2 的步骤 2 中执行完 Ping 命令所显示的信息有何不同？为什么会显示这样的信息？
   b) 对比该步骤中所抓取的 ICMP 报文和步骤 2 中所抓取的 ICMP 报文，有何不同？为什么出现这种区别？
   c) 在步骤 4 中，从 Host-8 发出的 ICMP 请求报文，是否到达了 Host-3？若到达了，尝试分析该报文的通信过程；若没有到达，说明在哪里被丢弃了？为什么被丢弃？（提醒：可结合 ARP 协议的应用进行分析）
9. 本实验任务 2 的步骤 5 中，在网络设备配置正常，各主机运行正常的情况下，使用主机 Host-8 Ping Net-A 部分中可配置未使用的任一 IP 地址：
   a) 执行该 Ping 命令后，屏幕上所显示的信息，与任务 2 的步骤 2 中执行完 Ping 命令所显示的信息有何不同？为什么会显示这样的信息？
   b) 对比该步骤中所抓取的 ICMP 报文和步骤 2 中所抓取的 ICMP 报文，有何不同？为什么出现这种区别？
   c) 在步骤 5 中，从 Host-8 发出的 ICMP 请求报文，传送到哪里就无法再进一步传送了？说明原因（提醒：可结合 ARP 协议的应用进行分析）
10. 本实验任务 2 的步骤 6 中，在网络设备配置正常，各主机运行正常的情况下，使用主机 Host-8 Ping Net-A 部分中可配置未使用的任一 IP 地址：
    a) 执行该 Ping 命令后，屏幕上所显示的信息，与任务 2 的步骤 2 中执行完 Ping 命令所显示的信息有何不同？为什么会显示这样的信息？
    b) 对比该步骤中所抓取的 ICMP 报文和步骤 2 中所抓取的 ICMP 报文，有何不同？为什么出现这种区别？
    c) 在步骤 6 中，从 Host-8 发出的 ICMP 请求报文，传送到哪里就无法再进一步传送了？说明原因（提醒：可结合 ARP 协议的应用进行分析）
11. 本实验任务 3 中，Traceroute 命令的作用是什么？其工作原理是啥？基于 Windows 操作系统也有一条类似的命令，它的名字是什么？
12. 本实验任务 3 的步骤 2 中，在使用主机 Host-8 对主机 Host-1 进行 Traceroute 路由测试时：

a) 执行该 trace 命令后，屏幕上所显示的信息？其含义是什么？
b) 对比该步骤中所抓取的 ICMP 报文和步骤 2 中所抓取的 ICMP 报文，有何不同？ICMP 报文类型是什么？为什么出现这种区别？
c) 在本步骤中，从 Host-8 发出的 ICMP 请求报文是什么类型？共发出几个 ICMP 请求报文？每一条 ICMP 请求报文分别传送到哪里？说明原因（提醒：可结合 Trace 命令的工作原理进行分析）

13. 本实验任务 3 的步骤（3）中，根据自己的实际操作结果，结合表 3-7 的内容，对抓包点 1 处所抓取的 ICMP 报文进行分析，并汇报给老师。
14. 本实验任务 3 的步骤（4）中，根据自己的实际操作结果，结合表 3-8 的内容，对抓包点 2 处所抓取的 ICMP 报文进行分析，并汇报给老师。
15. 本实验任务 3 的步骤（5）中，根据自己的实际操作结果，结合表 3-9 的内容，对抓包点 3 处所抓取的 ICMP 报文进行分析，并汇报给老师。
16. 本实验任务 3 的步骤（6）中，根据自己的实际操作结果，结合表 3-10 的内容，对抓包点 4 处所抓取的 ICMP 报文进行分析，并汇报给老师。
17. 本实验任务 3 的步骤（7）中，根据自己的实际操作结果，结合表 3-11 的内容，对抓包点 5 处所抓取的 ICMP 报文进行分析，并汇报给老师。