

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

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

(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
```

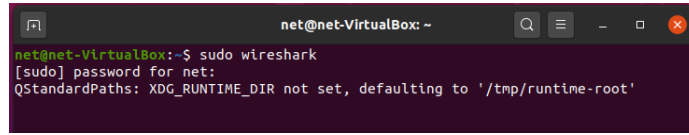


图 3-1 在终端启动 Wireshark

(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。

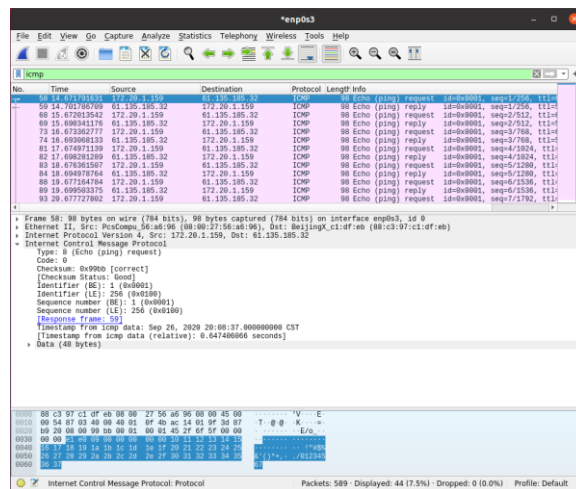


图 3-2 ICMP 报文

(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

(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。

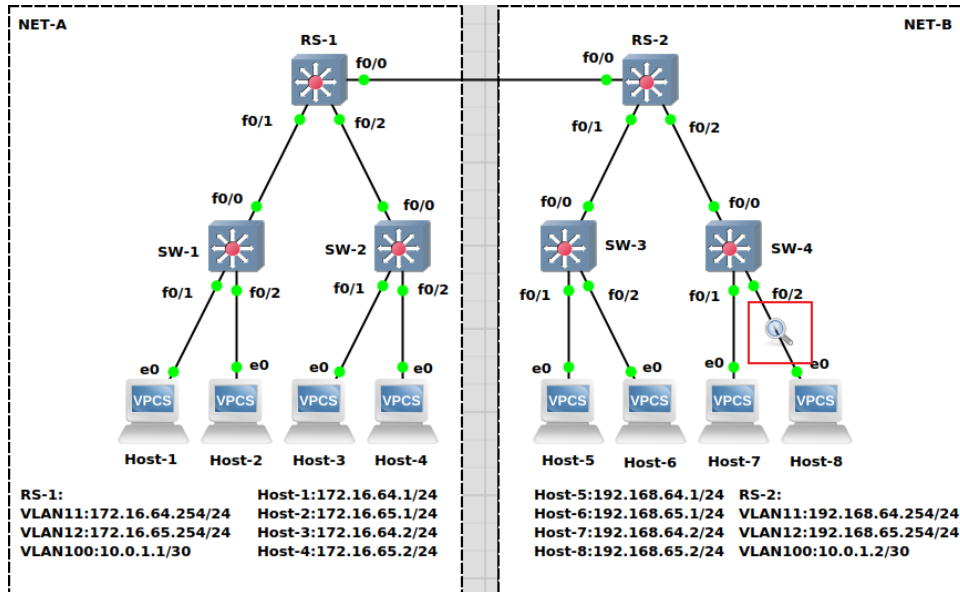


图 3-3 设置抓包点

(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

(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。

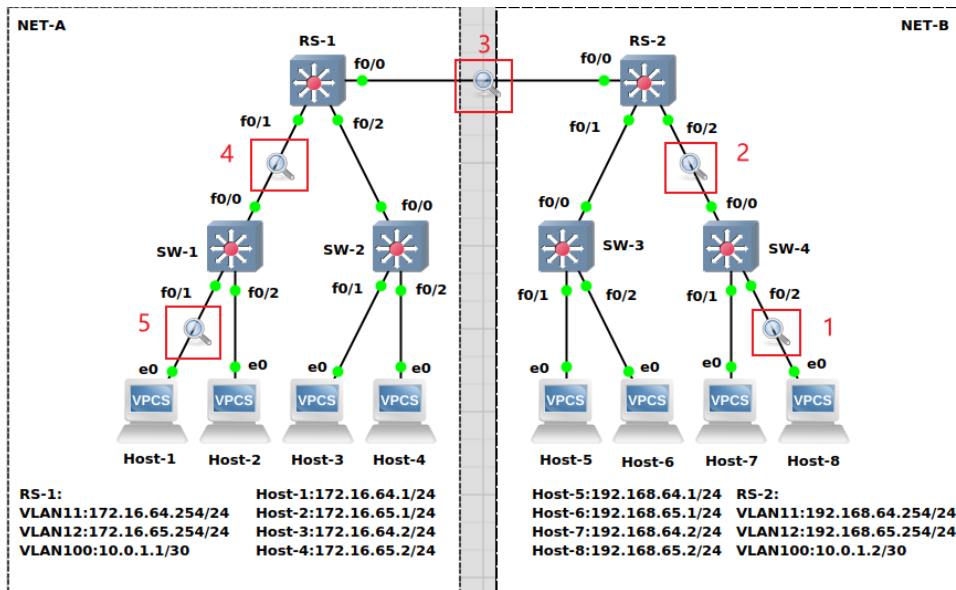


图 3-4 设置抓包点

(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。

```
Host-8> trace
trace HOSTI [OPTION ...]
Print the path packets take to the network HOSTI. HOSTI can be an ip address or name.
Options:
  -P protocol    Use IP protocol in trace packets
                  1 - icmp, 17 - udp (default), 6 - tcp
  -m ttl         Maximum ttl, default 8
Notes: 1. Using names requires DNS to be set.
       2. Use Ctrl+C to stop the command.
Host-8> trace 172.16.64.1 -P 1
trace to 172.16.64.1, 8 hops max (ICMP), press Ctrl+C to stop
 1  192.168.65.254   8.340 ms  9.646 ms  9.537 ms
 2  10.0.1.1       20.599 ms 20.924 ms 31.765 ms
 3  172.16.64.1   45.760 ms 41.183 ms 42.875 ms
Host-8>
```

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

实验考核分为【实验随堂查】和【实验线上考】两个部分。

实验随堂查：每个实验设置 3-5 考核点。完成实验任务后，任课教师随机选择一个考核点，学生现场进行演示和汇报讲解。

实验线上考：每个实验设置 5-10 个客观题。通过线上考核平台（课堂派）进行作答。

1、实验随堂查

本实验随堂查设置 4 个考核点，具体如下。

考核点 1：完成 ICMP 报文结构的分析。

考核点 2: 完成 ICMP 报文类型的分析。

考核点 3: 完成 PING 通信分析。

考核点 4: 完成 TRACEROUTE 通信分析。

2、实验线上考

本实验线上考共 10 题，其中单选 3 题、多选 2 题、判断 3 题、填空 2 题。