

## 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
//在本机上对 www.baidu.com 进行 PING 操作
ping www.baidu.com
```

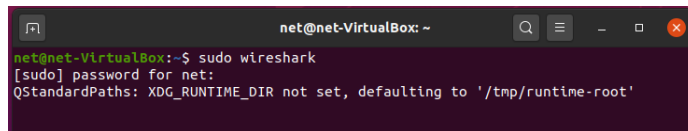


图 3-1 在终端启动 Wireshark

(2) 查看 ICMP 报文结构

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

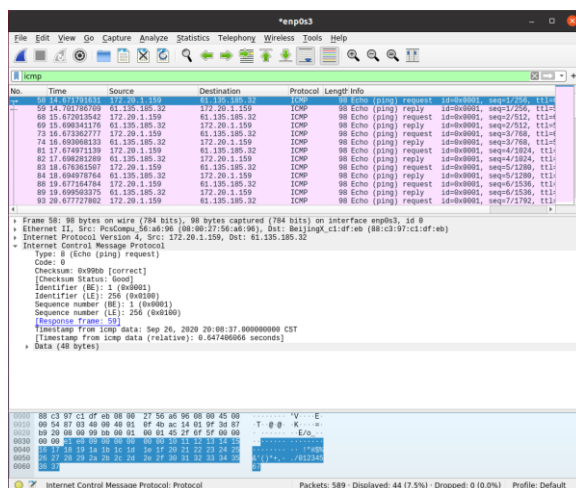


图 3-2 ICMP 报文

(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

在园区网中，使用主机 Host-8 对 NET-A 网络中的主机 Host-1、Host-2、Host-3、Host-4 进行连通性测试，并将测试结果填入表 3-2 中。

表 3-2 ICMP 回显请求和回显应答报文信息

报文分析点	源主机	目的主机	type	code	Identifier(BE) Identifier(LE)	Sequence(BE) Sequence(LE)	通信结果
1	Host-8	Host-1					
	Host-1	Host-8					
2	Host-8	Host-2					
	Host-2	Host-8					
3	Host-8	Host-3					
	Host-3	Host-8					
4	Host-8	Host-4					
	Host-4	Host-8					

(2) 设置测试环境

为了获取更多样的 ICMP 报文，调整主机实现测试环境。具体的调整如下：

①关闭主机 Host-1

②将主机 Host-4 的 IP 地址修改为 172.20.1.31/24，网关为 172.20.1.1

(3) 设置抓包点，启动 Wireshark 进行抓包

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。

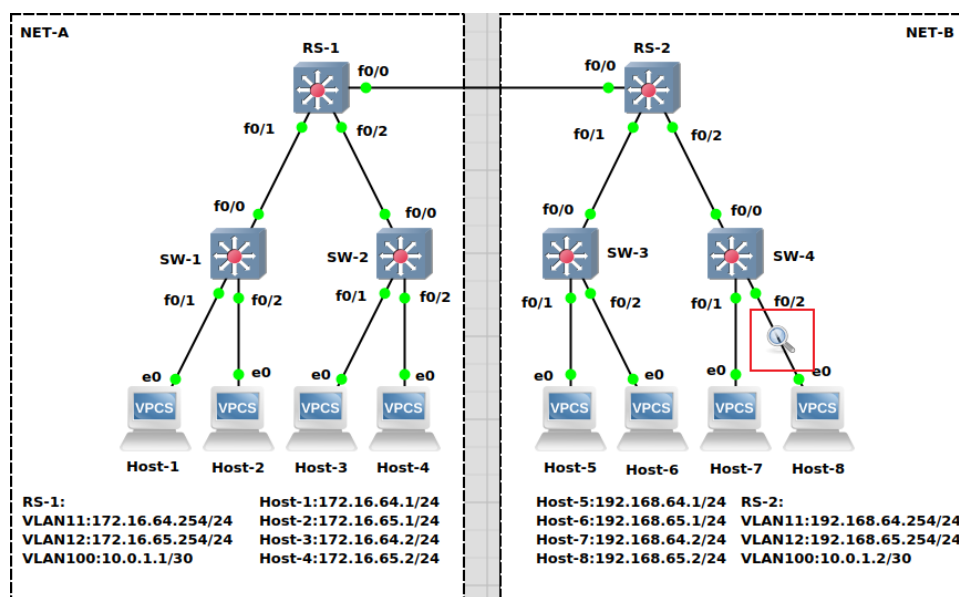


图 3-3 设置抓包点

(4) 基于 Host-8 进行通信测试，具体的通信测试如下：

- ①Host-8 主机 PING 主机 Host-1，此时主机 Host-1 已关机
- ②Host-8 主机 PING 主机 Host-2，此时主机 Host-2 正常
- ③Host-8 主机 PING 主机 Host-3，PING 时需指定 TTL 值为 1，此时主机 Host-3 正常
- ④Host-8 主机 PING 主机 Host-4 新的 IP 地址，此时主机 Host-4 正常，但无法连通

**参考命令：**

---

```
//设置 PING 命令的 TTL 值为 1
Host-8> PING 172.16.64.2 -T 1
```

---

(5) 分析 ICMP 报文

对 (4) 中获取的 ICMP 报文信息进行分析，将分析结果填写到表 3-3 中。

表 3-3 ICMP 报文信息

报文分析点	源主机	目的主机	type	code	Identifier(BE) Identifier(LE)	Sequence(BE) Sequence(LE)	通信结果
1	Host-8	Host-1					
	Host-1	Host-8					
2	Host-8	Host-2					
	Host-2	Host-8					
3	Host-8	Host-3					
	RS-2	Host-8					
4	Host-8	Host-4					
	RS-2	Host-8					

**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。

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

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

**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
```

---

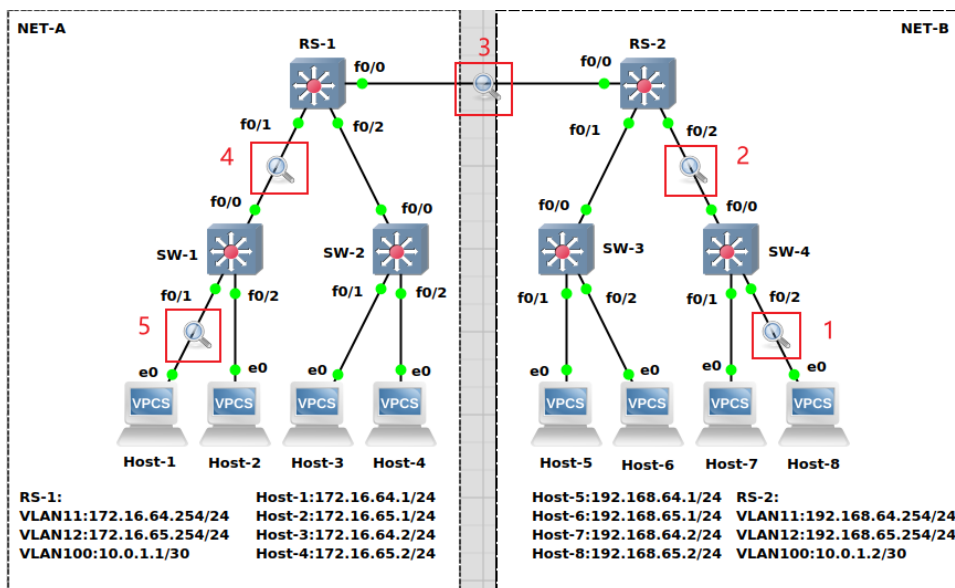


图 3-4 设置抓包点

```

Host-8
Trying 127.0.0.1...
Connected to localhost.
Escape character is '^]'.

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  10.240 ms  9.715 ms  10.375 ms
 2  10.0.1.1      18.449 ms 30.264 ms 29.847 ms
 3  * * *
 4  172.16.64.1   24.753 ms 20.634 ms  9.348 ms
    
```

图 3-5 Traceroute 路由测试

(3) 记录抓包点 1 的 ICMP 报文信息

对抓包点 1 获取的 ICMP 报文进行分析，将分析结果填入表 3-4-1 中。

表 3-4-1 抓包点 1 报文信息

报文分析点	源 IP 地址	目的 IP 地址	源 MAC	目的 MAC	TTL	Type	Code
1	192.168.65.2	172.16.64.1					
	192.168.65.254	192.168.65.2					
2	192.168.65.2	172.16.64.1					
	10.0.1.1	192.168.65.2					
3	192.168.65.2	172.16.64.1					
	172.16.64.1	192.168.65.2					

(4) 记录抓包点 2 的 ICMP 报文信息

对抓包点 2 获取的 ICMP 报文进行分析，将分析结果填入表 3-4-2 中。

表 3-4-2 抓包点 2 报文信息

报文分析点	源 IP 地址	目的 IP 地址	源 MAC	目的 MAC	TTL	type	code
1	192.168.65.2	172.16.64.1					
	192.168.65.254	192.168.65.2					
2	192.168.65.2	172.16.64.1					
	10.0.1.1	192.168.65.2					
3	192.168.65.2	172.16.64.1					
	172.16.64.1	192.168.65.2					

(5) 记录抓包点 3 的 ICMP 报文信息

对抓包点 3 获取的 ICMP 报文进行分析，将分析结果填入表 3-4-3 中。

表 3-4-3 抓包点 3 报文信息

报文分析点	源 IP 地址	目的 IP 地址	源 MAC	目的 MAC	TTL	type	code
1	192.168.65.2	172.16.64.1					
	10.0.1.1	192.168.65.2					
2	192.168.65.2	172.16.64.1					
	172.16.64.1	192.168.65.2					

(6) 记录抓包点 4 的 ICMP 报文信息

对抓包点 4 获取的 ICMP 报文进行分析，将分析结果填入表 3-4-4 中。

表 3-4-4 抓包点 4 报文信息

报文分析点	源 IP 地址	目的 IP 地址	源 MAC	目的 MAC	TTL	type	code
1	192.168.65.2	172.16.64.1					
	172.16.64.1	192.168.65.2					

(7) 记录抓包点 5 的 ICMP 报文信息

对抓包点 5 获取的 ICMP 报文进行分析，将分析结果填入表 3-4-5 中。

表 3-4-5 抓包点 5 报文信息

报文分析点	源 IP 地址	目的 IP 地址	源 MAC	目的 MAC	TTL	type	code
1	192.168.65.2	172.16.64.1					
	172.16.64.1	192.168.65.2					

(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 Trace route 的工作原理。

## 七、实验考核

### 1、任务说明

使用 GNS3 完成 ICMP 协议的分析。

### 2、任务要求

要求 1：完成 ICMP 报文结构的分析；

要求 2：完成 ICMP 报文类型的分析；

要求 3：完成 PING 通信分析。

### 3、考核要求

题目 1：使用 Wireshark 抓取报文，在主机 Host-3 上 Ping 主机 Host-6，请提交【ICMP 报文】内容截图。

题目 2：分析【ICMP 报文】结构，请填写以下信息。

“Type”的字段大小：\_\_\_\_\_，含义：\_\_\_\_\_；

“Code”的字段大小：\_\_\_\_\_，含义：\_\_\_\_\_；

“Checksum”的字段大小：\_\_\_\_\_，含义：\_\_\_\_\_；

“Identifier”的字段大小：\_\_\_\_\_，含义：\_\_\_\_\_；

“Sequence”的字段大小：\_\_\_\_\_，含义：\_\_\_\_\_。

题目 3：请简述 ICMP 的协议类型。

题目 4：请简要说明 ICMPv4 和 ICMPv6 报文有什么相同点和不同点。