# 实验四 ICMP 协议和IP 数据报分片分析

## 【实验目的】

1. 理解 ICMP 协议报文类型和格式；

2. 理解 ping 命令的工作原理；

3. 理解 traceroute 的工作原理；

4. 理解 IP 协议报文类型和格式。

## 【实验环境】

与因特网连接的计算机，操作系统为Windows，安装有Wireshark、IE 等软件。

## 【实验内容】

1. 使用 wireshark 抓包软件分析ICMP 协议报文的类型；

2. 分析 ping 命令的工作原理；

3. 分析 tracert 命令的工作原理；

4. 使用 wireshark 抓包软件分析IP 协议报文以及报文分片。

## 【实验步骤】

**1. 分析 ICMP 协议**

步骤1：在 PC1 运行 Wireshark，开始截获报文，为了只截获和实验内容有关的报文，将

Wireshark 的 Captrue Filter 设置为“No Broadcast and no Multicast”；

步骤2：在 PC1 以 202.120.111.3 为目标主机，在命令行窗口执行 Ping 命令，要求ping

通8 次；

**【答**】：Ping 命令为：

将命令行窗口进行截图：

**【答**】：

步骤3：停止截获报文，分析截获的结果，回答下列问题：

（1）将抓包结果进行截图（要求只显示 ping 的数据包）：

（2）截获的 ICMP 报文有几种类型？分别是：

**【答**】：

（3）分析截获的 ICMP 报文，按下表要求，将各字段信息填入表中，要求填写前4 个报文的信息。

**【答**】：

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **报文号** | **源IP** | **目的IP** | **报文格式** | | | | | |
| **类型** | **代码** | **标识** | | **序列号** | |
| **BE** | **LE** | **BE** | **LE** |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |

（4）查看ping 请求信息，ICMP 的type是 \_\_\_ \_\_\_。和code是 \_\_\_\_。并截图。

**【答**】：

（5）查看相应得ICMP 响应信息，ICMP 的type 是\_\_\_ \_\_\_和code 是 \_\_\_\_。并截图。

**【答**】：

（6）若要只显示ICMP的echo响应数据包，显示过滤器的规则为\_\_ \_\_\_.并根据过滤规则进行抓包截图。

**【答**】：

7) 若要只显示ICMP的echo请求数据包，显示过滤器的规则为\_\_\_ \_\_\_. 并根据过滤规则进行抓包截图。

**【答**】：

**2. 分析traceroute 的工作原理**

步骤1：在 PC1 上运行 Wireshark 开始截获报文；

步骤2：在PC1上执行Tracert命令，如：tracert 202.120.111.3；将命令窗口进行截图；

步骤3：在wireshark里设置显示过滤器为icmp；

步骤4：停止截获报文，分析截获的报文，回答下列问题：

（1）截获了报文中哪几种 ICMP 报文？其类型码和代码各为多少？

**【答**】：

|  |  |  |
| --- | --- | --- |
| **ICMP 报文** | **类型码** | **代码** |
|  |  |  |
|  |  |  |
|  |  |  |

（2）在截获的报文中，哪些是超时报告报文，请截图显示所有超时报文并指出超时报告报文的源地址分别是多少？

**【答**】：

（3）查看 ICMP echo 分组 ，是否这个分组和前面使用 ping 命令的ICMP echo 一样？若不一样，请分析使用tracert 命令后收到的分组里TTL 值的变化规律。

**【答**】：

（4）对照 ICMP 协议，分析一下ICMP 超时报告分组比ICMP echo 分组多包含的信息有哪些？

**【答**】：

（5）对于ICMP超时报告分组，找出与命令提示窗口截图中的第六跳路由器的接口IP地址为多少？在wireshark抓包图中截图与第五跳路由器的接口IP地址对应的部分并截图。

**【答**】：

**3. IP协议分析**

步骤1：分别在 PC1 和 PC2 上运行 wireshark，开始截获报文，为了只截获和实验内容有

关的报文，将 wireshark 的 Captrue Filter 设置为“No Broadcast and no Multicast”；

步骤2： PC1 ping PC2；

步骤3：停止截获报文，分析截获的结果，回答下列问题：

（1）任取一个有 IP 协议的数据报并截图。

**【答**】：

（2）分析该 IP 协议的报文格式，完成下表。

表 IP 协议

|  |  |  |
| --- | --- | --- |
| **字段** | **报文信息** | **说明** |
| **版本** |  |  |
| **头长** |  |  |
| **服务类型** |  |  |
| **总长度** |  |  |
| **标识** |  |  |
| **标志** |  |  |
| **片偏移** |  |  |
| **生存周期** |  |  |
| **协议** |  |  |
| **校验和** |  |  |
| **源地址** |  |  |
| **目的地址** |  |  |

**4. IP数据报分片实验**

步骤1：在 PC1、PC2 两台计算机上运行 Wireshark，为了只截获和实验有关的数据报，设

置 Wireshark 的捕获条件为对方主机的 IP 地址的icmp协议；

步骤2：在 PC1 上执行如下 Ping 命令，向主机 PC2 发送大小为7000个字节的数据报文；

步骤3：停止截获报文并回答下列问题：

（1）以太网的最大传输单元(MTU)是多少？怎么计算得出的？

**【答**】：

（2）分析截获的报文，将属于同 ICMP 请求报文的分片找出来并从wireshark 中截图，主机PC1 向主机 PC2 发送的 ICMP 请求报文分成了\_\_\_\_个分片。

（3）ICMP 报文各分片的数据长度是多少？在wireshark 里截图显示。

**【答**】：

（4）若要让主机PC1向主机PC2发送的数据分为2个分片，则 Ping 命令中的报文长度应为多大范围？为什么？

**【答】：**