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。

										*enp0s3								
Eile	<u></u> Edit	View	<u>G</u> o	Capture	Analyze	Statist	cs Te	lephony	Win	eless <u>T</u> oo	ls <u>H</u> elp							
		1			X 🕻	9			Ŧ	± 💷		Q (11				
II ic	mp																×	v +
No.	т	ime		Source			Destina	tion		Protoco	l Lengt	Info						-
<pre></pre>	59 1 68 1 73 1 73 1 81 1 82 1 83 1 84 1 83 1 84 1 93 2 93 2 93 2 93 2 93 2 93 2 93 2 93 2	4.7017 5.6720 6.6733 6.6733 6.6733 8.6949 7.6749 8.6763 8.6949 8.6763 8.6949 8.6777 8.98 8.6777 8.98 8.6777 8.98 8.6777 8.98 8.6777 8.98 8.6777 8.98 8.6777 8.98 8.6777 8.98 8.6777 8.98 8.6777 8.98 8.6771 8.98 8.5771 8.98 8.577 8.98 8.5771 8.98 8.577 8.98 8.577 8.98 8.577 8.98 8.577 8.98 8.577 8.98 8.577 8.98 8.577 8.98 8.577 8.577 8.577 8.577 8.577 8.578 8.577 8.578 8.577 8.578 8.577 8.578 8.577 8.578 8.577 8.578 8.577 8.578 8.577 8.578 8.577 8.578 8.577 8.578 8.5778 8.578 8.578 8.5778 8.578 8.578 8.578 8.578 8.578 8.578 8.5778	86709 13542 52777 66133 71139 81289	61.133 172.22 11.02 61.133 172.22 11.02 61.133 172.22 11.02 61.03 172.22 10.02 61.03 172.22 10.0	186 32 1.1.50 1.85 32 1.85 32 1.85 32 1.85 32 1.85 32 1.85 32 1.85 32 1.1.59 1.85 32 1.1.59 1.85 32 1.1.59 (784 bi 1.55 32 1.1.59 (784 bi 1.55 32 4. Src: rotocol quest) ct] 001) (9x8001 56 (8x01) a: Sep 2 ta (rela	ts) 98 6 (98:00 172.26.3) 30) 30) 5, 2928 5, 2928 1, 2028 1, 2028 2, 2028 1,	72.20 11.135 17.2.20 11.135 17.2.20 11.135 17.2.20 11.135 17.2.20 11.135 17.2.20 11.135 11.135 17.2.20 11.135 11.1	1.159 185.32 185.32 185.32 185.32 185.32 185.32 185.32 1.159 185.32 1.159 185.32 captur 185.32 captur 37.0000 6666 s	ed (7), Ds 1.135	CCMP ICMP ICMP ICMP ICMP ICMP ICMP ICMP	99 96 96 96 96 98 98 98 98 98 98 98 98 98 98 98 98 98	Echo Echo Echo Echo Echo Echo Echo Echo	(ping) (p	reply request reply request reply request reply request reply request . id 0 97:c1:df	11-0x0001. 11-0x0	eeq=1/256, seq=2/512, seq=2/512, seq=3/768, seq=3/768, seq=3/768, seq=4/1024 seq=4/1024 seq=6/1503 seq=7/1792	ttl= ttl= ttl= , ttl , ttl , ttl , ttl , ttl	
0000 0010 0020 0030 0040 0050 0050	88 (90 5 99 (16 26 36	23 97 0 54 87 6 20 08 6 90 91 0 17 18 1 27 28 2	1 df 3 40 0 99 9 1a 9 2a	eb 08 00 00 49 01 00 00 01 10 1c 1c 2b 2c 20	27 56 9f 4b 90 91 90 99 1e 1f 2e 2f	a6 96 06 ac 14 01 45 2f 6f 10 11 12 20 21 22 30 31 32	00 45 9f 3d 5f 00 13 14 23 24 33 34	00 87 00 15 35	T • 0	0 K E/o_	E- =- \$3, 45							
0	In	ternet (Contro	l Messag	e Protocol	Protoco				Pack	ets: 589	 Displ 	ayed: 4	4 (7.5%) -	Dropped: 0 (0	1.0%) Profil	e: Defa	ult

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
Туре		
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。

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

表 3-2 ICMP 回显请求和回显应答报文信息

(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											
	源主机 IP	目的主机 IP	type	code	Identifier	Sequence					
请求											
报文											
	请求内容(data):										
	源主机 IP	目的主机 IP	type	code	Identifier	Sequence					
响应											
报文											
	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										
	源主机 IP	目的主机 IP	type	code	Identifier	Sequence					
请求											
报文	请求内容(data):										
	源主机 IP	目的主机 IP	type	code	Identifier	Sequence					
响应											
	响应内容(data):		1			L					

(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。

寿	3-5	ICMP	回显请:	龙和同员	品应答报	☆信息
-10	5-5	101111		1 V I H I U U		人口心

	Host-8 Ping 172.16.64.100											
	源主机 IP	目的主机 IP	type	code	Identifier	Sequence						
请求												
1XX	请求内容(data):											
	源主机 IP	目的主机 IP	type	code	Identifier	Sequence						
响应												
报义	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										
	源主机 IP	目的主机 IP	type	code	Identifier	Sequence					
请求											
叔又	请求内容(data):										
	源主机 IP	目的主机 IP	type	code	Identifier	Sequence					
响应											
」 和文	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。

Ē		Host-8		Q				
Host-8> trace								
trace <u>HOST</u> [OP] Print the pat name.	<u>ION</u>] h packets tak	e to the network <u>HOST</u> .	<u>HOST</u> can	be	an ip	add	ress	ог
options: -P <u>protoc</u> -m <u>ttl</u>	<u>ol</u> Use IP 1 - i Maximum	<u>protocol</u> in trace pack cmp, 17 - udp (default 1 <u>ttl</u> , default 8	ets), 6 - tc	P				
Notes: 1. Usi 2. Use	ng names requ Ctrl+C to st	ires DNS to be set. op the command.						
Host-8> trace f trace to 172.16 1 192.168.69 2 10.0.1.1 3 172.16.64	72.16.64.1 -P .64.1, 8 hops .254 8.340 20.599 ms 2 1 45.760 ms	1 max (ICMP), press Ctr ms 9.646 ms 9.537 ms 0.924 ms 31.765 ms 41.183 ms 42.875 ms	l+C to st	ор				
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。

报文 相似类	源 IP 地址	目的 IP 地址	TTL	Туре	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						

表 3-7 抓包点1的报文分析结果

(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。

报文 相似类	源 IP 地址	目的 IP 地址	TTL	Туре	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						

表 3-8 抓包点 2 的报文分析结果

(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。

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

表 3-9 抓包点 3 的报文分析结果

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	Туре	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。

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

表 3-11 抓包点 5 的报文分析结果

(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 Tracer oute 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

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: 完成表 3-1 的填写,并提交填写完的表格截图和对应的数据报文截图。

题目 2: 完成表 3-2、3-3、3-6 的填写,并提交填写完的表格截图和对应的数据报文截 图。

题目 3: 完成表 3-7、3-9、3-11 的填写,并提交填写完的表格截图和对应的数据报文截 图。

题目 4: 请简述 ICMP 的协议类型。

题目 5: 请结合任务 3 的实验结果,分析说明 Traceroute 的工作原理。