



西安电子科技大学网信院

《组网与运维》

线上实验报告

班级：

姓名：

学号：

日期：

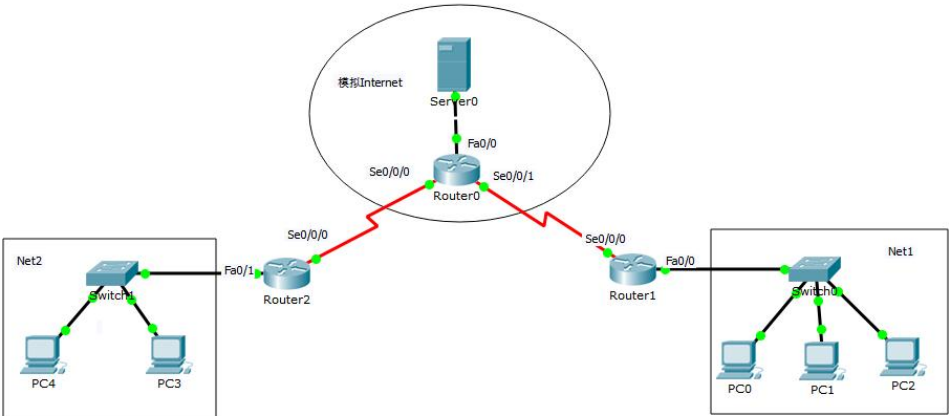
VPN与NAT协议分析

一、实验目的

- 1. 理解 VPN 使用的 IP 隧道技术的工作原理。
- 2. 理解 NAT 技术的工作原理。

二、实验步骤

- 1. 给出实验中用到的拓扑图



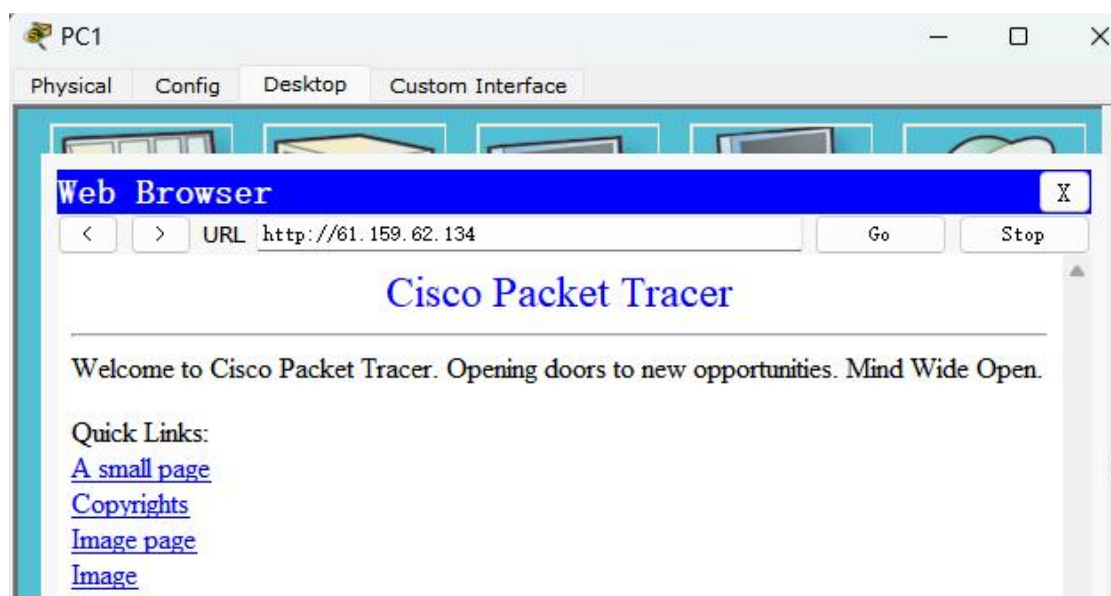
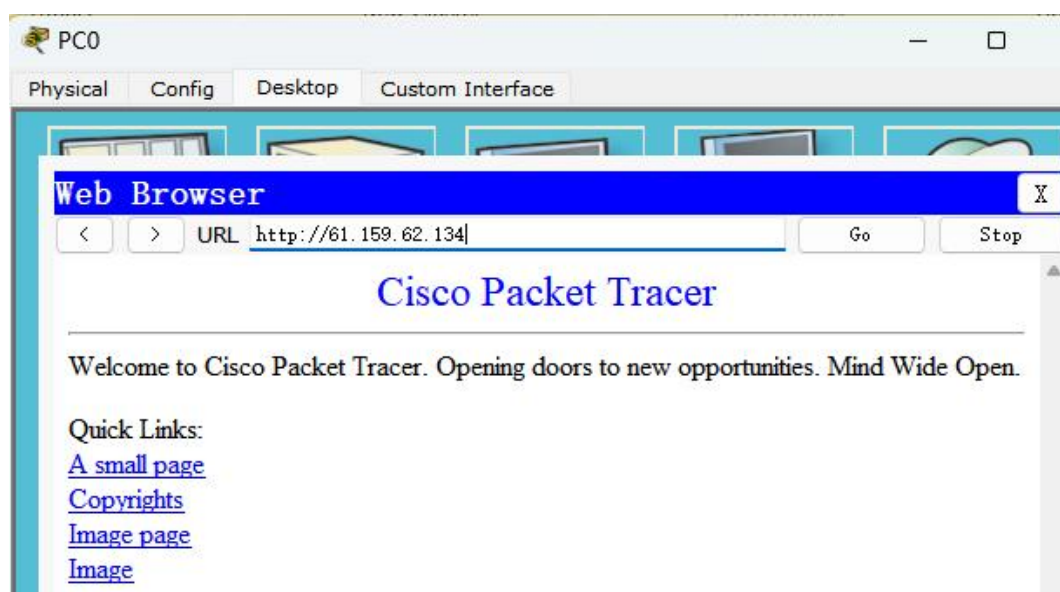
- 2. 给出实验中使用的 IP 配置表

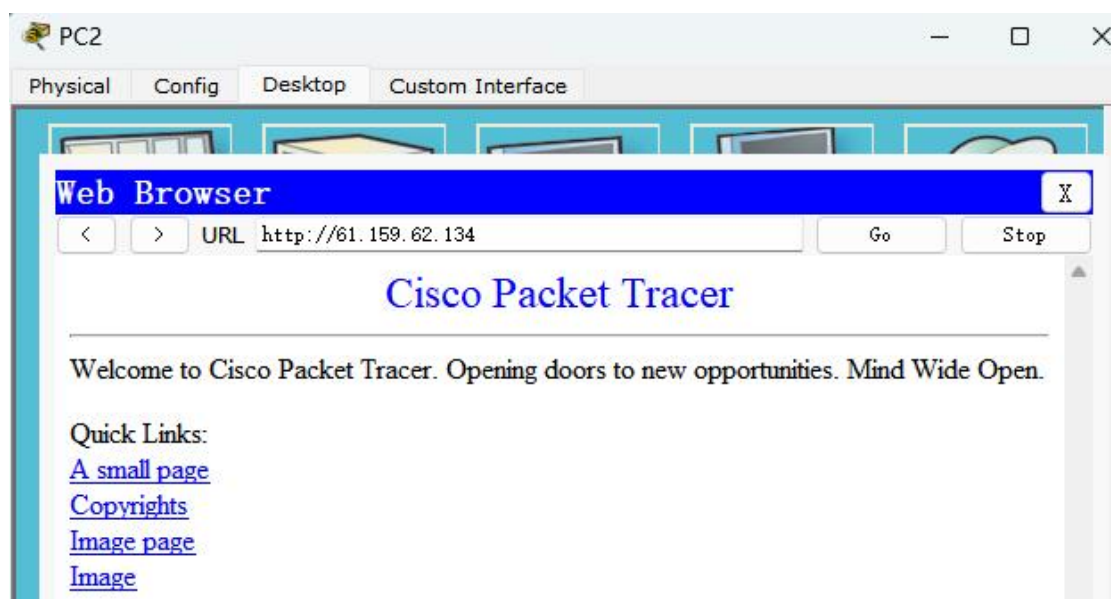
设备	接口	IP 地址	掩码	默认网关
PC0	Fa0	192. 168. 1. 1	255. 255. 255. 0	192. 168. 1. 254
PC1	Fa0	192. 168. 1. 2	255. 255. 255. 0	192. 168. 1. 254
PC2	Fa0	192. 168. 1. 3	255. 255. 255. 0	192. 168. 1. 254
PC3	Fa0	192. 168. 2. 2	255. 255. 255. 0	192. 168. 2. 254
PC4	Fa0	192. 168. 2. 1	255. 255. 255. 0	192. 168. 2. 254
Router0	Fa0/0	61. 159. 62. 12	255. 0. 0. 0	---
	Se0/0/0	158. 22. 120. 169	255. 255. 255. 0	---
	Se0/0/1	158. 22. 130. 33	255. 255. 255. 0	---
Router1	Fa0/0	192. 168. 1. 254	255. 255. 255. 0	---
	Se0/0/0	158. 22. 130. 34	255. 255. 255. 0	---
Router2	Se0/0/0	158. 22. 120. 168	255. 255. 255. 0	---
	Fa0/0	61. 159. 62. 12	255. 0. 0. 0	---
Server	Fa0	61. 159. 62. 134	255. 0. 0. 0	61. 159. 62. 12

3. 任务一：观察学习 NAT 的工作原理

✧ 步骤 1：分别在 PC0-PC2 中访问 Web 服务器。

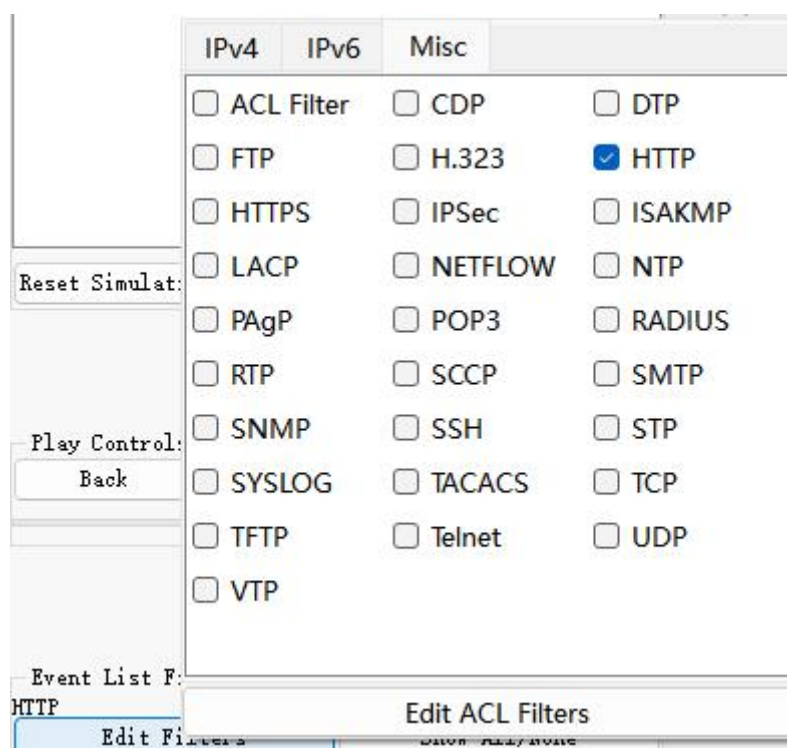
在实时模式的逻辑空间中单击 PC0, 在 Desktop 中单击 Web Browser 按钮（网页浏览器），在 URL 地址栏中输入 `http://61.159.62.134` (Server0 的 IP 地址) 并按 Enter 键。此时可以看到打开的网页。按同样的方法，分别在 PC1 和 PC2 中访问 Web 服务器。
















✧ 步骤 2: 观察 NAT 路由器对数据包的处理方法。

进入 Simulation(模拟)模式, 设置 Event List Filters (事件列表过滤器) 只显示 HTTP 事件。在 PC0 的 Web Browser 中重新刷新网页, 并逐步单击 Capture/Forward 按钮, 以控制模拟进程, 此时可观察到 HTTP 报文的传输往返过程。当出现 Buffer Full 窗口时, 停止模拟过程。



Event List					
Vis.	Time(sec)	Last Device	At Device	Type	Info
	0.309	--	PC0	HTTP	
	0.313	--	PC0	HTTP	
	0.314	PC0	Switch0	HTTP	
	0.315	Switch0	Router1	HTTP	
	0.316	Router1	Router0	HTTP	
	0.317	Router0	Server0	HTTP	
	0.318	Server0	Router0	HTTP	
	0.319	Router0	Router1	HTTP	
	0.320	Router1	Switch0	HTTP	
	0.321	Switch0	PC0	HTTP	



使用检查工具 (Inspect) 打开 Router1 的 NAT 地址转换表 (NAT Table)。

NAT Table for Router1				
Protocol	Inside Global	Inside Local	Outside Local	Outside Global
tcp	158.22.130.34:1025	192.168.1.1:1025	61.159.62.134:80	61.159.62.134:80
tcp	158.22.130.34:1027	192.168.1.1:1026	61.159.62.134:80	61.159.62.134:80
tcp	158.22.130.34:1027	192.168.1.1:1027	61.159.62.134:80	61.159.62.134:80
tcp	158.22.130.34:1044	192.168.1.1:1044	61.159.62.134:80	61.159.62.134:80
tcp	158.22.130.34:1024	192.168.1.2:1025	61.159.62.134:80	61.159.62.134:80

在 Event List 窗口中找到 At Device 为 Router1 的事件，单击其彩色正方形。分别选择 Inbound PDU Details 和 Outbound PDU Details 选项卡，以查看和对比 PDU 内容的区别。可以发现在 Inbound PDU 中，该 PDU 的源目 IP 地址分别为 192.168.1.1 和 61.159.62.134。而在 Outbound PDU 中，PDU 的源目 IP 地址已经更改为 158.22.130.34 和 61.159.62.134。同时对照 NAT 地址转换表，观察源和目的端口的转换规律。

PDU Information at Device: Router1

OSI Model

Inbound PDU Details

Outbound PDU Details

PDU Formats

Ethernet II

0	4	8	14	19	Bytes
PREAMBLE: 101010...1011			DEST MAC: 0010.1191.A201	SRC MAC: 0004.9AAD.A614	
TYPE: 0x800		DATA (VARIABLE LENGTH)		FCS: 0x0	

IP

0	4	8	16	19	31	Bits
4	IHL	DSCP: 0x0	TL: 122			
ID: 0x3c			0x2	0x0		
TTL: 128		PRO: 0x6	CHKSUM			
SRC IP: 192.168.1.1						
DST IP: 61.159.62.134						
OPT: 0x0				0x0		
DATA (VARIABLE LENGTH)						

PDU Information at Device: Router1

OSI Model

Inbound PDU Details

Outbound PDU Details

PDU Formats

HDLC

0	8	16	32	32+x	48+x	56+x	F
FLG: 011 1	ADR: 0x8f	CONTROL: 0x0	DATA: (VARIABLE LENGTH)		FCS: 0x0	FLG: 011 1	

IP

0	4	8	16	19	31	Bits
4	IHL	DSCP: 0x0	TL: 122			
ID: 0x3c			0x2	0x0		
TTL: 127		PRO: 0x6	CHKSUM			
SRC IP: 158.22.130.34						
DST IP: 61.159.62.134						
OPT: 0x0				0x0		
DATA (VARIABLE LENGTH)						

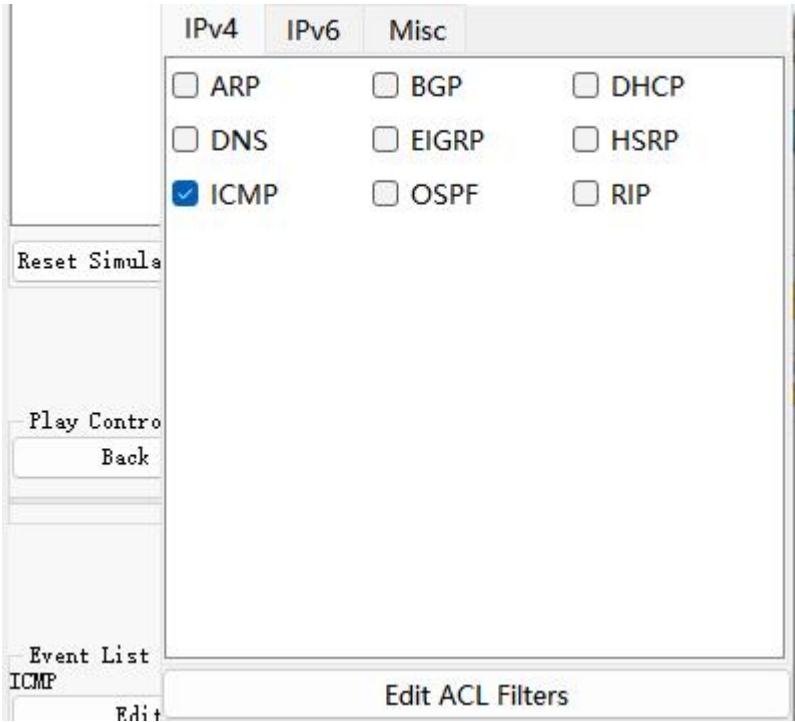
4. 任务二：观察学习 VPN 工作原理

✧ 步骤 1：初始化模拟。

进入实时模式。单击 Add Simple PDU(添加简单 PDU) 按钮，然后分别单击 PC0(源站点)和 PC3(目的站点)，则 PC0 将快速向 PC3 发送一个包含 ICMP 报文的 IP 数据报。该过程的主要目的是初始化 VPN 连接。

✧ 步骤 2：观察 VPN 的隧道技术。

切换到模拟模式，并设置 Event List Filters(事件列表过滤器) 只显示 ICMP 事件。



单击 Auto Capture/Play(自动捕获/播放)或者 Capture/Forward 按钮，以运行模拟，并捕获事件和数据包。此时,可观察到 ICMP 数据报的转发过程。

Event List					
Vis.	Time(sec)	Last Device	At Device	Type	Info
	0.000	--	PC0	ICMP	
	0.001	PC0	Switch0	ICMP	
	0.002	Switch0	Router1	ICMP	
	0.003	Router1	Router0	ICMP	
	0.004	Router0	Router2	ICMP	
	0.005	Router2	Switch1	ICMP	
	0.006	Switch1	PC3	ICMP	
	0.006	Switch1	PC4	ICMP	

Simulation Panel					
Event List					
Vis.	Time(sec)	Last Device	At Device	Type	Info
	0.006	Switch1	PC3	ICMP	
	0.006	Switch1	PC4	ICMP	
	0.007	PC3	Switch1	ICMP	
	0.008	Switch1	Router2	ICMP	
	0.009	Router2	Router0	ICMP	
	0.010	Router0	Router1	ICMP	
	0.011	Router1	Switch0	ICMP	
	0.012	Switch0	PC0	ICMP	

在 Event List 窗口中找到 At Device 为 Router1 的事件，单击其彩色正方形。分别选择 Inbound PDU Details 和 Outbound PDU Details 选项卡，查看和对比 PDU 内容的区别。可以发现在 Inbound PDU 中，该 PDU 的源目 IP 地址分别为 192.168.1.1(PC0 的 IP 地址)和 192.168.2.2(PC3 的 IP 地址)。而在 Outbound PDU 中，PDU 的源目 IP 地址已经更改为 158.22.130.34(Router1 的 Se0/0/0 的 IP 地址)和 158.22.120.168(Router2 的 Se0/0/0 的 IP 地址)，并且原 IP 包已经被重新封装在新的 IP 包中，这就是隧道技术的工作原理。

PDU Information at Device: Router1

OSI Model

Inbound PDU Details

Outbound PDU Details

PDU Formats

Ethernet II

0	4	8	14	19	Bytes
PREAMBLE: 101010...1011		DEST MAC: 0010.1191.A201		SRC MAC: 0004.9AAD.A614	
TYPE: 0x800	DATA (VARIABLE LENGTH)			FCS: 0x0	

IP

0	4	8	16	19	31	Bits
4	IHL	DSCP: 0x0	TL: 28			
ID: 0x56			0x0	0x0		
TTL: 255		PRO: 0x1	CHKSUM			
SRC IP: 192.168.1.1						
DST IP: 192.168.2.2						
OPT: 0x0				0x0		
DATA (VARIABLE LENGTH)						

PDU Information at Device: Router1

OSI Model Inbound PDU Details Outbound PDU Details

PDU Formats

0

8

16

32

32+x

48+x

56+x

E

FLG:
011
1

ADR:
0x8f

CONTROL:
0x0

DATA: (VARIABLE
LENGTH)

FCS:
0x0

FLG:
011
1

0

4

8

16

19

31

Bits

4

IHL

DSCP: 0x0

TL: 20

ID: 0x38

0x0

0x0

TTL: 255

PRO: 0x32

CHKSUM

SRC IP: 158.22.130.34

DST IP: 158.22.120.168

OPT: 0x0

0x0

DATA (VARIABLE LENGTH)

在 Event List 窗口中找到 At Device 为 Router2 的事件，单击其彩色正方形。分别选择 Inbound PDU Details 和 Outbound PDU Details 选项卡，以查看和对比 PDU 内容的区别。可以发现在 Inbound PDU 中，该 PDU 的源目 IP 地址分别为 158.22.130.34(Router1 的 Se0/0/0 的 IP 地址)和 158.22.120.168(Router2 的 Se0/0/0 的 IP 地址)。而在 Outbound PDU 中，PDU 的源目 IP 地址已经更改为 192.168.1.1(PC0 的 IP 地址)和 192.168.2.2(PC3 的 IP 地址)，这说明 PC0 发送的 IP 包被 Router2 重新解封出来。

PDU Information at Device: Router2

OSI Model

Inbound PDU Details

Outbound PDU Details

PDU Formats

HDLC

0	8	16	32	32+x	48+x	56+x	E
FLG: 011 1	ADR: 0x8f	CONTROL: 0x0	DATA: (VARIABLE LENGTH)	FCS: 0x0	FLG: 011 1		

IP

0	4	8	16	19	31	Bits
4	IHL	DSCP: 0x0	TL: 20			
ID: 0x38		0x0	0x0			
TTL: 254		PRO: 0x32	CHKSUM			
SRC IP: 158.22.130.34						
DST IP: 158.22.120.168						
OPT: 0x0				0x0		
DATA (VARIABLE LENGTH)						

PDU Information at Device: Router2

OSI ModelInbound PDU DetailsOutbound PDU Details

PDU Formats

Ethernet II

0	4	8	14	19	Bytes
PREAMBLE: 101010...1011		DEST MAC: 00D0.BA0A.7884		SRC MAC: 0001.C95A.8202	
TYPE: 0x800	DATA (VARIABLE LENGTH)			FCS: 0x0	

IP

0	4	8	16	19	31	Bits
4	IHL	DSCP: 0x0	TL: 28			
ID: 0x56		0x0	0x0			
TTL: 253	PRO: 0x1	CHKSUM				
SRC IP: 192.168.1.1						
DST IP: 192.168.2.2						
OPT: 0x0				0x0		
DATA (VARIABLE LENGTH)						

三、思考与总结

1. 在任务一中,Router1 如何区分 Server0 返回给不同主机的 HTTP 报文?

答: NAT 服务器 (Router1) 通过不同的端口号来识别不同的主机的报文。

2. 在任务二中, VPN 中采用隧道技术的原因是什么?。

答: 由于 Net1 和 Net2 都是使用私有地址, 因此无法直接通过 Internet 进行通信: 采用隧道技术可以方便地将源目地址转换为全局地址, 而且到达目标路由器后, 也很容易获得真正目标主机的 IP 地址。

3. Net1 网络和 Net2 网络的 IP 地址能否编在同一段?

答: 不行, 这样容易造成两个网段间主机的 IP 地址发生冲突。

4. 实验过程中还遇到什么问题, 如何解决的? 通过该实验有何收获?

本次实验学习了 VPN 和 NAT 协议分析有关知识, 了解了一些原理。