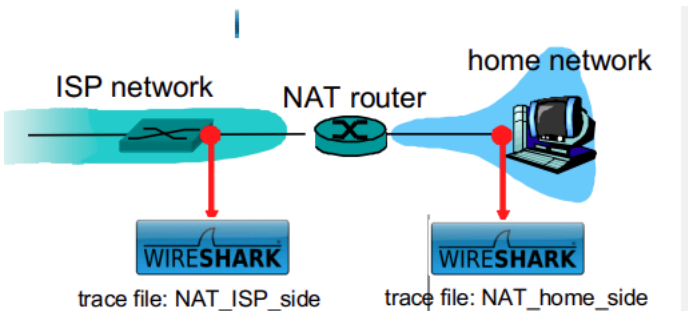


计算机网络 课程实验报告

学号：202000130143	姓名： 郑凯饶	班级： 2020 级 1 班
实验题目：NAT		
实验学时：2	实验日期： 2022-5-3	
实验目的： 学习 NAT 协议		
硬件环境： Dell Latitude 5411 Intel (R) Core(TM) i5-10400H CPU @ 2.60GHz (8GPUs), ~2.6GHz		
软件环境： Windows 10 家庭中文版 64 位（10.0，版本 18363） Wireshark-win64-3.6.2		
实验步骤与内容：		
1. 问题：		
(1) 客户端的 IP 地址。		
(2) 设置过滤器：http && ip.addr == 64.233.169.104		
(3) 选择客户端于 7.109267 时间向服务器的 HTTP GET 报文，回答其 IP 及端口信息。		
(4) 何时接收到 Google 服务器回复的 200 OK HTTP 消息，回答其 IP 及端口信息。		
(5) 客户端何时发送 TCP SYN 报文建立连接发送了在 7.109267 发送的 GET 请求。回答 IP 及端口信息。还有响应的 ACK 报文。		
(6) 找到（3）中客户端发送的 GET 请求，它什么时间出现，回答 IP 及端口信息。和（3）有哪些不同？		
(7) GET 请求中字段是否更改，IP 数据包中 Version, Header Length, Flags, Checksum 等，它们的变化说明了什么。		
(8) 接收第一条 HTTP 200 OK 在什么时间？回答 IP 及端口。和（4）有哪些不同？		
(9) （5）中 SYN 和 TCP ACK 报文出现在什么位置？回答 IP 及端口，有哪些不同？		
(10) 作出 NAT 转换表。		
2. 阐述基本方法		
 <p>Figure 1: NAT trace collection scenario</p>		
NAT 原理：对于有网络访问需求而内部使用私有地址的网络（home network），在组织的出口位置部署 NAT 网关，在报文离开私网进入公网（ISP network）时，将源 IP 替换为公网地址，通常是接口设备的接口地址。一个来自外部的访问到达时网关将目的地址		

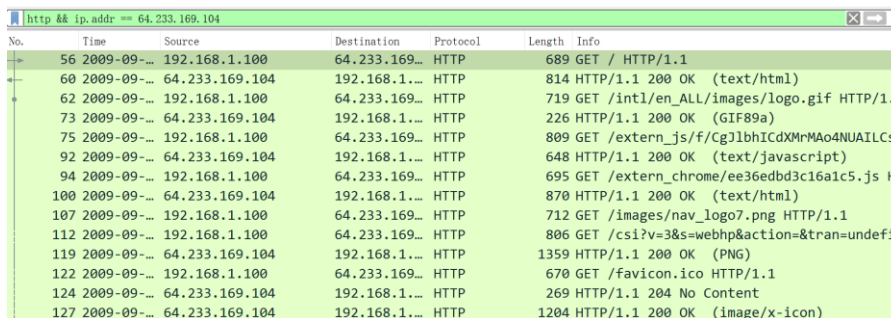
转为私网的源主机 IP.

要点:

- 【1】 双向流量必须经过 NAT 网关;
- 【2】 网络访问只能由私网侧发起, 公网无法主动访问私网主机, 起到防火墙作用;
- 【3】 NAT 网关的存在对于通信双方是保持透明的;
- 【4】 NAT 网关需要保存一张 NAT 转换表。

3. 实验结果展示与分析

(1) Source Address: 192.168.1.100



No.	Time	Source	Destination	Protocol	Length	Info
56	2009-09-...	192.168.1.100	64.233.169...	HTTP	689	GET / HTTP/1.1
60	2009-09-...	64.233.169.104	192.168.1.100	HTTP	814	HTTP/1.1 200 OK (text/html)
62	2009-09-...	192.168.1.100	64.233.169...	HTTP	719	GET /intl/en_ALL/images/logo.gif HTTP/1.1
73	2009-09-...	64.233.169.104	192.168.1.100	HTTP	226	HTTP/1.1 200 OK (GIF89a)
75	2009-09-...	192.168.1.100	64.233.169...	HTTP	809	GET /extern_js/f/CgJlbhICdXMmMAo4NUAILCsu HTTP/1.1
92	2009-09-...	64.233.169.104	192.168.1.100	HTTP	648	HTTP/1.1 200 OK (text/javascript)
94	2009-09-...	192.168.1.100	64.233.169...	HTTP	695	GET /extern_chrome/ee36edbd3c16a1c5.js HTTP/1.1
100	2009-09-...	64.233.169.104	192.168.1.100	HTTP	870	HTTP/1.1 200 OK (text/html)
107	2009-09-...	192.168.1.100	64.233.169...	HTTP	712	GET /images/nav_logo7.png HTTP/1.1
112	2009-09-...	192.168.1.100	64.233.169...	HTTP	806	GET /csi?v=3&s=webhp&action=&tran=undefin HTTP/1.1
119	2009-09-...	64.233.169.104	192.168.1.100	HTTP	1359	HTTP/1.1 200 OK (PNG)
122	2009-09-...	192.168.1.100	64.233.169...	HTTP	670	GET /favicon.ico HTTP/1.1
124	2009-09-...	64.233.169.104	192.168.1.100	HTTP	269	HTTP/1.1 204 No Content
127	2009-09-...	64.233.169.104	192.168.1.100	HTTP	1204	HTTP/1.1 200 OK (image/x-icon)

(2) 设置如上图。

(3) Source Address: 192.168.1.100

Destination Address: 64.233.169.104

Source Port: 4335

Destination Port: 80

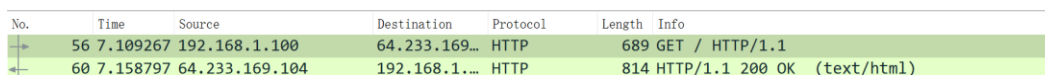
(4) ACK 紧随其后:

Source Address: 64.233.169.104

Destination Address: 192.168.1.100

Source Port: 80

Destination Port: 4335



No.	Time	Source	Destination	Protocol	Length	Info
56	7.109267	192.168.1.100	64.233.169...	HTTP	689	GET / HTTP/1.1
60	7.158797	64.233.169.104	192.168.1.100	HTTP	814	HTTP/1.1 200 OK (text/html)

(5) No. 53 为 SYN, No. 54 为 SYN ACK

No. 53: Source Address: 192.168.1.100

Destination Address: 64.233.169.104

Source Port: 4335

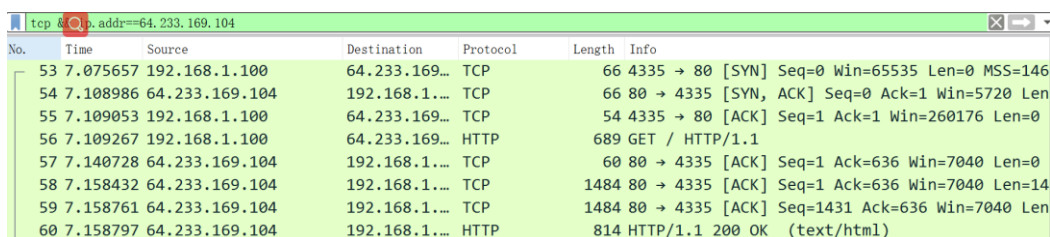
Destination Port: 80

No. 54: Source Address: 64.233.169.104

Destination Address: 192.168.1.100

Source Port: 80

Destination Port: 4335



No.	Time	Source	Destination	Protocol	Length	Info
53	7.075657	192.168.1.100	64.233.169...	TCP	66	4335 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=146
54	7.108986	64.233.169.104	192.168.1.100	TCP	66	80 → 4335 [SYN, ACK] Seq=0 Ack=1 Win=5720 Len=0
55	7.109053	192.168.1.100	64.233.169...	TCP	54	4335 → 80 [ACK] Seq=1 Ack=1 Win=260176 Len=0
56	7.109267	192.168.1.100	64.233.169...	HTTP	689	GET / HTTP/1.1
57	7.140728	64.233.169.104	192.168.1.100	TCP	60	80 → 4335 [ACK] Seq=1 Ack=636 Win=7040 Len=0
58	7.158432	64.233.169.104	192.168.1.100	TCP	1484	80 → 4335 [ACK] Seq=1 Ack=636 Win=7040 Len=14
59	7.158761	64.233.169.104	192.168.1.100	TCP	1484	80 → 4335 [ACK] Seq=1431 Ack=636 Win=7040 Len=0
60	7.158797	64.233.169.104	192.168.1.100	HTTP	814	HTTP/1.1 200 OK (text/html)

(6) 根据传送内容判断, NAT_ISP_side 中 85 对应 (3) 中客户端 GET 请求。

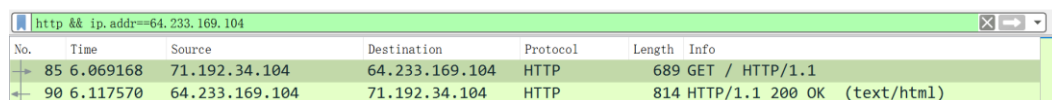
Source Address: 71.192.34.104

Destination Address: 64.233.169.104

Source Port: 4335

Destination Port: 80

源地址变更。



No.	Time	Source	Destination	Protocol	Length	Info
85	6.069168	71.192.34.104	64.233.169.104	HTTP	689	GET / HTTP/1.1
90	6.117570	64.233.169.104	71.192.34.104	HTTP	814	HTTP/1.1 200 OK (text/html)

(7) HTTP 消息无更改, IP 数据报变化。

Source Address : 192.168.1.100→71.192.34.104, 进行 NAT 转化

Header Checksum : 0xa94a→0x022f, 首部字段发生变化

Time to Live: 128→127, 传输过程中时间消耗

(8) ACK 同样紧随其后。

Source Address: 64.233.169.104

Destination Address: 71.192.34.104

Source Port: 80

Destination Port: 4335

目的地址不同。

(9) No. 82 为 SYN

Source Address: 71.192.34.104

Destination Address: 64.233.169.104

Source Port: 4335

Destination Port: 80

No. 83 为 SYN ACK

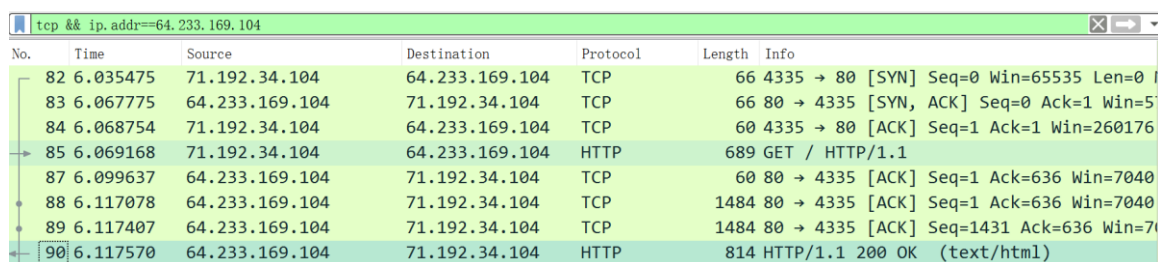
Source Address: 64.233.169.104

Destination Address: 71.192.34.104

Source Port: 80

Destination Port: 4335

目的端口不同。



No.	Time	Source	Destination	Protocol	Length	Info
82	6.035475	71.192.34.104	64.233.169.104	TCP	66	4335 → 80 [SYN] Seq=0 Win=65535 Len=0
83	6.067775	64.233.169.104	71.192.34.104	TCP	66	80 → 4335 [SYN, ACK] Seq=0 Ack=1 Win=5
84	6.068754	71.192.34.104	64.233.169.104	TCP	60	4335 → 80 [ACK] Seq=1 Ack=1 Win=260176
85	6.069168	71.192.34.104	64.233.169.104	HTTP	689	GET / HTTP/1.1
87	6.099637	64.233.169.104	71.192.34.104	TCP	60	80 → 4335 [ACK] Seq=1 Ack=636 Win=7040
88	6.117078	64.233.169.104	71.192.34.104	TCP	1484	80 → 4335 [ACK] Seq=1 Ack=636 Win=7040
89	6.117407	64.233.169.104	71.192.34.104	TCP	1484	80 → 4335 [ACK] Seq=1431 Ack=636 Win=7
90	6.117570	64.233.169.104	71.192.34.104	HTTP	814	HTTP/1.1 200 OK (text/html)

(10) NAT 转换表:

WAN: 192.168.1.100:4335 ↔ LAN: 71.192.34.104:4335

结论分析与体会:

这次实验我们学习了 NAT。NAT 帮助我们解决了 IPV4 地址资源不足的问题,但是它也有一些弊端,如破坏了 IP 协议端到端的通信能力。在 P2P 应用中一个用户的主机既是下载的客户,也为其他客户提供数据,是一种混合 C/S 混合的模型,而 NAT 使得通信会话只能单方面发起,极大限制了 P2P。因此,NAT 穿透技术诞生了。网络的世界多么奇妙,以后在内网搭建服务时应该还有机会回顾 NAT。