

计算机网络实验报告

课程名称 计算机网络 成绩评定

实验项目名称 NAT 协议 指导教师 张伟

实验项目编号 实验 8 实验项目类型 实验地点

学生姓名 密语 学号 202200460104

学院 网络空间安全 专业 网络空间安全

实验时间 2024 年 5 月 7 日

一、实验目的

理解 NAT 协议的运作。

二、实验步骤与结果

任务一：

1. 客户端的 IP 地址是多少？

1	0.000000	192.168.1.100	10.119.240.64	SNMP	120	get-requ
2	1.124897	192.168.1.100	68.87.71.230	DNS	91	Standard
3	1.138265	68.87.71.230	192.168.1.100	DNS	211	Standard
4	1.140302	192.168.1.100	74.125.91.113	TCP	66	4330 → 80
5	1.207818	74.125.91.113	192.168.1.100	TCP	66	80 → 4330
6	1.207873	192.168.1.100	74.125.91.113	TCP	54	4330 → 80
7	1.208040	192.168.1.100	74.125.91.113	TCP	1035	4330 → 80

由图可知，客户端的 IP 地址为 192.168.1.100

2. 客户端实际上与几个不同的 Google 服务器通信，以实现“安全浏览”（请参阅任务三）。

提供主要 Google 网页的服务器地址是 64.233.169.104，为了仅仅显示客户端的请求和服务器的响应，请在 Wireshark 过滤器输入以下过滤条件“http && ip.addr == 64.233.169.104 ”（不包括引号）。请截图当前显示的内容。

NAT_home_side.pcap

文件(F) 编辑(E) 视图(V) 跳转(G) 捕获(C) 分析(A) 统计(S) 电话(Y) 无线(W) 工具(T) 帮助(H)

http && ip.addr == 64.233.169.104

No.	Time	Source	Destination	Protocol	Length	Info
56	7.109267	192.168.1.100	64.233.169.104	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)
62	7.281399	192.168.1.100	64.233.169.104	HTTP	719	GET /intl/en_ALL/images/logo.gif HTTP/1.1
73	7.349451	64.233.169.104	192.168.1.100	HTTP	226	HTTP/1.1 200 OK (GIF89a)
75	7.370185	192.168.1.100	64.233.169.104	HTTP	809	GET /extern_js/f/CgJlbhICdXMrMAo4NUAILCswDjgHLCswFjgQLCswFzgDLCswGDgELCswGTg: HTTP/1.1
92	7.448649	64.233.169.104	192.168.1.100	HTTP	648	HTTP/1.1 200 OK (text/javascript)
94	7.492324	192.168.1.100	64.233.169.104	HTTP	695	GET /extern_chrome/ee36edbd3c16a1c5.js HTTP/1.1
100	7.537353	64.233.169.104	192.168.1.100	HTTP	870	HTTP/1.1 200 OK (text/html)
107	7.652836	192.168.1.100	64.233.169.104	HTTP	712	GET /images/nav_logo7.png HTTP/1.1
112	7.682361	192.168.1.100	64.233.169.104	HTTP	806	GET /csi?v=3&s=webhp&action=&tran=undefined&e=17259,21588,21766,21920&ei=250: HTTP/1.1
119	7.685786	64.233.169.104	192.168.1.100	HTTP	1359	HTTP/1.1 200 OK (PNG)
122	7.709490	192.168.1.100	64.233.169.104	HTTP	670	GET /favicon.ico HTTP/1.1
124	7.737783	64.233.169.104	192.168.1.100	HTTP	269	HTTP/1.1 204 No Content
127	7.763501	64.233.169.104	192.168.1.100	HTTP	1204	HTTP/1.1 200 OK (image/x-icon)

3. 请选择在 7.109267 s 时间的客户端发送到 Google 服务器（其 IP 地址为 IP 地址 64.233.169.104）的 HTTP GET。承载此 HTTP GET 的 IP 数据报上的源 IP 地址和目标 IP 地址以及 TCP 源端口和目标端口是什么？

源 IP 地址是 192.168.1.100，目的 IP 地址是 64.233.169.104

TCP 源端口是 4335，目标端口是 80

4. 对于前一问发送的 HTTP GET 消息，在什么时间客户端从 Google 服务器收到对应的状态码 200、状态 OK 的 HTTP 响应消息？携带状态码 200、状态 OK 的 HTTP 响应消息的 IP 数据报上的源和目标 IP 地址以及 TCP 源和目标端口是什么？

7.158797s 的时候收到响应消息，源 IP 地址是 64.233.169.104，目标 IP 地址是 192.168.1.100，

TCP 源端口是 80，目标端口是 4335

5. 回想一下，在将 GET 请求发送到 HTTP 服务器之前，TCP 必须首先使用三次 SYN/ACK 消息建立连接。在什么时间客户端发送了含有 TCP SYN 的报文建立连接消息，以后续用于发送在 7.109267 s 的 GET 请求？TCP SYN 报文的源 IP 地址和目标 IP 地址以及源端口和目标端口是什么？在什么时间客户端收到了对应的 SYN-ACK 报文？此 SYN-ACK 报文的源和目标 IP 地址以及源端口和目标端口是什么？（注意你需要清除在第 2 题中的过滤器表达式并且输入“tcp”（不含引号）表达式，仅仅显示 TCP 报文消息。）

7.075657 s

源 IP 地址是 192.168.1.100，目的 IP 地址是 64.233.169.104

TCP 源端口是 4335，目标端口是 80

在 7.108986 s 收到了 SYN-ACK 报文

源 IP 地址是 64.233.169.104，目标 IP 地址是 192.168.1.100，TCP 源端口是 80，目标端口是 4335

任务二：

1. 在 NAT_ISP_side 跟踪文件中，找到跟刚才客户端 7.109267s 同样目的地发送的 HTTP GET 消息（这个时间是在 NAT_home_side 跟踪文件中记录的时间）。该消息何时出现在 NAT_ISP_side 跟踪文件中？承载此 HTTP GET 消息的 IP 数据报的源和目标 IP 地址以及 TCP 源和目标端口是什么？

6.069168 s 时出现在 NAT_ISP_side 跟踪文件中

源 IP 地址：71.192.34.104，源端口：4335

目的 IP 地址：64.233.169.104 目的端口：80

2. 与任务一的第 3 问中找到的 HTTP GET 消息相比，此 HTTP GET 消息中的某些字段发生了变化。试分析 IP 层中的所有字段，找到发生改变的字段，说明这些字段的值由原来的什么数值改变成了现在的什么数值，并解释改变的原因。

<pre>Internet Protocol Version 4, Src: 192.168.1.100, Dst: 64.233.169.104 0100 = Version: 4 0101 = Header Length: 20 bytes (5) > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT) Total Length: 675 Identification: 0xa2ac (41644) > 010. = Flags: 0x2, Don't fragment ...0 0000 0000 0000 = Fragment Offset: 0 Time to Live: 128 Protocol: TCP (6) Header Checksum: 0xa94a [validation disabled] [Header checksum status: Unverified] Source Address: 192.168.1.100 Destination Address: 64.233.169.104</pre>	<pre>Internet Protocol Version 4, Src: 71.192.34.104, Dst: 64.233.169.104 0100 = Version: 4 0101 = Header Length: 20 bytes (5) > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT) Total Length: 675 Identification: 0xa2ac (41644) > 010. = Flags: 0x2, Don't fragment ...0 0000 0000 0000 = Fragment Offset: 0 Time to Live: 127 Protocol: TCP (6) Header Checksum: 0x022f [validation disabled] [Header checksum status: Unverified] Source Address: 71.192.34.104 Destination Address: 64.233.169.104</pre>
--	--

Checksum 字段改变了，由原来的 0xa94a 变成了 0x022f

源 IP 地址不同，由 192.168.1.100 变成了 71.192.34.104

原因：进行了 NAT 地址转换导致源 IP 地址发生改变，由于源 IP 地址改变了，导致校验和字段发生变化。

3. 在 NAT_ISP_side 跟踪文件中，从 Google 服务器收到的第一条 HTTP 200 OK 消息在什么时间？携带此 HTTP 200 OK 消息的 IP 数据报上的源 IP 和目标 IP 地址以及 TCP 源和目标端口是什么？与你在任务一的第 4 问对于回答的 NAT_home_side 的结果相比，哪些字段相同，哪些字段不同？

<pre>Internet Protocol Version 4, Src: 64.233.169.104, Dst: 192.168.1.100 0100 = Version: 4 0101 = Header Length: 20 bytes (5) > Differentiated Services Field: 0x20 (DSCP: CS1, ECN: Not-ECT) Total Length: 800 Identification: 0xf61e (63006) > 000. = Flags: 0x0 ...0 0000 0000 0000 = Fragment Offset: 0 Time to Live: 50 Protocol: TCP (6) Header Checksum: 0xe33b [validation disabled] [Header checksum status: Unverified] Source Address: 64.233.169.104 Destination Address: 192.168.1.100</pre>	<pre>Internet Protocol Version 4, Src: 64.233.169.104, Dst: 71.192.34.104 0100 = Version: 4 0101 = Header Length: 20 bytes (5) > Differentiated Services Field: 0x20 (DSCP: CS1, ECN: Not-ECT) Total Length: 800 Identification: 0xf61e (63006) > 000. = Flags: 0x0 ...0 0000 0000 0000 = Fragment Offset: 0 Time to Live: 51 Protocol: TCP (6) Header Checksum: 0x3a20 [validation disabled] [Header checksum status: Unverified] Source Address: 64.233.169.104 Destination Address: 71.192.34.104</pre>
---	---

6.117570s

源 IP 地址：64.233.169.104，源端口：80

目的 IP 地址：71.192.34.104，目的端口：4335

校验和 checksum 字段、目的 IP 地址字段和生存时间不同，其余字段都相同。

4. 在 NAT_ISP_side 跟踪文件中，跟任务一的第 5 问相同的客户端到服务器 TCP SYN 报文段和服务器到客户端 TCP SYN-ACK 报文段是在什么时间出现的？这两个报文段的源 IP 和目标 IP 以及源端口和目标端口是什么？与你在任务一的第 5 问的回答相比，哪些字段相同，哪些字段与不同？

6.035475 s 和 6.067775 s

SYN: 源 IP 地址和端口: 71.192.34.104, 4335 目的 IP 地址和端口: 64.233.169.104, 80

ACK: 源 IP 地址和端口: 64.233.169.104, 80 目的 IP 地址和端口: 71.192.34.104, 4335

SYN 的源 IP 地址和 ACK 的目的 IP 地址变了，校验和变了，其余字段都没变。

5. 使用对于之前问题的回答，做出类似图 1 的 NAT 转换表（NAT translation table）

NAT translation table	
WAN side	LAN side
71.192.34.104,4335	192.168.1.100,4335

任务三：

1. 除了上面提到的 HTTP GET 消息和 HTTP 200 OK 消息以外，还与其他 Google 服务器有额外的连接，例如，在 NAT_home_side 跟踪文件中，分析时间为 1.572315s 的客户端到服务器 GET 消息，以及时间为 7.573305s 的 GET 消息。仔细研究这两个 HTTP 消息的使用，写出说明分别解释这两个消息的作用。

20 1.572315 192.168.1.100 74.125.106.31 HTTP 767 GET /safebrowsing/rd/goog-malware-shavar_s_15361-15365.15361-15365.: HTTP/1.1

访问的是 Google Safe Browsing API 服务，目的是保护用户免受恶意软件和不安全网站的威胁，实现安全浏览。

104 7.573305 192.168.1.100 74.125.91.113 HTTP 709 GET /generate_204 HTTP/1.1

GET /generate_204 是一个常见的网络请求，通常用于检查网络连接的状态。当设备连接到网络时，它可能会发送一个 HTTP GET 请求到 /generate_204 路径，以便检测网络连接是否正常工作。这个请求通常在设备连接到公共 Wi-Fi 网络或需要进行网络身份验证时触发。