|  |
| --- |
| 实验目的：  使用wireshark来跟踪NET协议  实验结果：   1. 客户端的 IP 地址是多少？   屏幕截图 2023-04-20 175054  屏幕截图 2023-04-20 175054  局域网ip：192.168.1.100  广域网ip:71.192.34.104  2、客户端实际上与几个不同的谷歌服务器进行通信，以实现“安全浏览”。（参见本实验室结尾的额外学分部分）。将提供主谷歌网页的主谷歌服务器有IP地址64.233.169.104。为了只显示那些包含从这个谷歌服务器发送的HTTP消息的帧,显示如下图所示：  屏幕截图 2023-04-20 175301   1. 现在考虑从时间7.109267从客户端发送到谷歌服务器（其IP地址为IP地址64.233.169.104）的HTTP GET。携带此HTTP GET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？   如下图所示：源地址：192.168.1.100目标地址：64.233.169.104  源端口：4335 目标端口：80  屏幕截图 2023-04-20 194420   1. **从 Google 服务器收到的响应 200 OK HTTP 消息在什么时间？ 携带此 HTTP 200 OK 消息的 IP 数据报上的源和目的地 IP 地址以及 TCP 源、目的地端口是什么？**   如下图所示：时间 7.15  源地址：64.233.169.104目标地址：192.168.1.100  源端口：80 目标端口：4335  **屏幕截图 2023-04-20 194549**  **5.在 GET 命令发送到 HTTP 服务器之前，TCP 必须首先使用SYN/ACK 三次握手建立连接。客户机到服务器发送的 GET 在 7.109267 时发送的连接的TCP SYN段是在什么时间发送的？ TCP SYN 段的源和目的地 IP 地址以及源和目的地端口是什么？响应 SYN 发送的 ACK 的源和目的地 IP 地址和源和目的地端口是什么？客户端在什么时候收到这个ACK?**  **发送SYN的时间，源地址，目的地址，源端口号，目的端口号如第一个红框所示：**  **响应 SYN 发送的 ACK 如第二个红框所示：**  **屏幕截图 2023-04-20 195008**  **为什么局域网和广域网的时间不同？**  **6. 在NAT\_ISP\_side跟踪文件中，找到 HTTP GET 消息是从客户端发送到 Google 服务器的时间 7.109267（其中 t=7.109267 是将此发送的时间记录在 NAT\_home\_side跟踪文件中）。 此消息在什么时间出现在NAT\_ISP\_side跟踪文件中？ 携带此 HTTP GET 的 IP 数据图上的源和目的地 IP 地址以及 TCP 源和目的地端口（如NAT\_ISP\_side跟踪文件中的记录）是什么？ 这些字段中哪些领域相同，哪些与您对上述问题 3 的回答不同？**  **时间 6.069 源地址：71.192.34.104 目的地址：64.233.169.104**  **源端口：4335目的端口：80 源地址不同，校验和不同**  屏幕截图 2023-04-20 194456   1. **HTTP GET消息中的任何字段是否已更改？携带 HTTP GET 的 IP 数据图中的哪些字段已更改：版本、头长度、标志、检查表。 如果这些字段中的任何一个已更改，给出一个理由（在一句话中）说明该字段需要更改的原因**   **源地址发生改变，**  **因为校验和中包含源地址，故源地址发生改变会使校验和发生改变。**  **对比如下图所示：**  **广域网：屏幕截图 2023-04-20 200212 局域网：屏幕截图 2023-04-20 200228**   1. **在NAT\_ISP\_side跟踪文件中，从 Google 服务器收到的第一个 200 个 OK HTTP 消息在什么时间？ 携带此 HTTP 200 OK 消息的 IP 数据图上的源和目的地 IP 地址以及 TCP 源和目的地端口是什么？这些字段中哪些是相同的，哪些与您对上述问题 4 的回答不同？**   **时间：6.11 源目的地址和端口如红框所示：**  **屏幕截图 2023-04-20 194603**  **不同之处：目的地址**  **9.在NAT\_ISP\_side跟踪文件中，什么时候捕获了与上面问题五的段对应的客户端到服务器 TCP SYN 段和服务器对客户端 TCP ACK 段？这两个网段的源和目的地 IP 地址以及来源和目的地端口是什么？这些字段中哪些字段相同，哪些字段与您对上述问题 5 的回答不同？**  **捕获：6.035 syn ack:6.067**  **屏幕截图 2023-04-20 195038**  **SYN报文：源地址不同，SYN,ACK报文目的地址不同**  **10.使用您对上面 1-8 的答案，填写上述问题 1-8 中考虑的 HTTP 连接的 NAT 转换表项.**  **将广域网地址和局域网地址进行转换**  71.192.34.104, 4335 192.168.1.100, 4335 |