山东大学 计算机 学院

计算机网络 课程实验报告

学号：202400130240	姓名： 贾宗翰	班级： 24.6
实验题目：NAT		
实验学时：2h	实验日期： 2025.10.21	
实验目的： 研究 NAT 路由器的行为		
硬件环境： 联想拯救者		
软件环境： wireshark		

实验步骤与内容：

在本实验中，我们将研究 NAT 路由器的行为。此实验室将不同于我们的其他 Wireshark 实验室，在后者中，我们在单个 Wireshark 测量点捕获了跟踪文件。由于我们对在 NAT 设备的输入和输出端捕获数据包感兴趣，因此我们需要在两个位置捕获数据包。此外，由于许多学生无法轻松访问 NAT 设备或两台用于进行 Wireshark 测量的计算机，因此这不是一个学生可以轻松“现场”完成的实验室。因此，在本实验中，您将使用我们为您捕获的 Wireshark 跟踪文件。这应该是一个相对较短且简单的实验，因为 NAT 背后的概念并不难，但观察 NAT 的实际应用还是很好的。

在本实验中，我们将捕获包含从家庭网络内部的客户端到远程服务器的简单 HTTP GET 请求消息的数据包，以及来自该服务器的相应 HTTP 响应。在家庭网络中，家庭网络路由器提供 NAT 服务，如第 4 章所述。图 1 显示了我们的 Wireshark 跟踪收集场景。我们将在两个位置捕获数据包，因此本实验有两个跟踪文件： • 我们将捕获在 NATrouter 的局域网（LAN） 端接收的数据包。此 LAN 中的所有设备都有 192.168.10/24 的地址。此文件名为 nat-inside-wireshark-trace1-1.pcapng

由于我们还对分析 NAT 路由器在面向 Internet 的一端转发(和接收)的数据包感兴趣，因此我们将在路由器的 Internet 端收集第二个跟踪文件，如图 1 所示。此时由 Wireshark 捕获的从右侧主机发送到左侧服务器的数据包在到达第二个测量点时将进行 NAT 转换。此文件名为 nat-outside-wireshark-trace1-1.pcapng。

在图 1 所示的场景中，LAN 中的一台主机将向 IP 地址为 138.76.29.8 的 Web 服务器发送一个 HTTP GET 请求，该服务器将响应请求主机。当然，我们对 HTTP GET 请求本身并不真正感兴趣，而是 NAT 路由器如何将包含 GET 请求的数据报的 IP 地址和端口号更改为 NAT 路由器的 Internet 端（外部）的转发数据报中的地址和端口号。我们首先看一下 NAT 路由器的 LAN 端发生了什么。打开 nat-inside-wireshark-trace1-1.pcapng 跟踪文件。在此文件中，您应该会看到一个发往 IP 地址为 138.76.29.8 的外部 Web 服务器的 HTTP GETrequest，以及随后的 HTTP 响应消息（“200 OK”）。跟踪文件中的两条消息都是在路由器的 LAN 端捕获的。

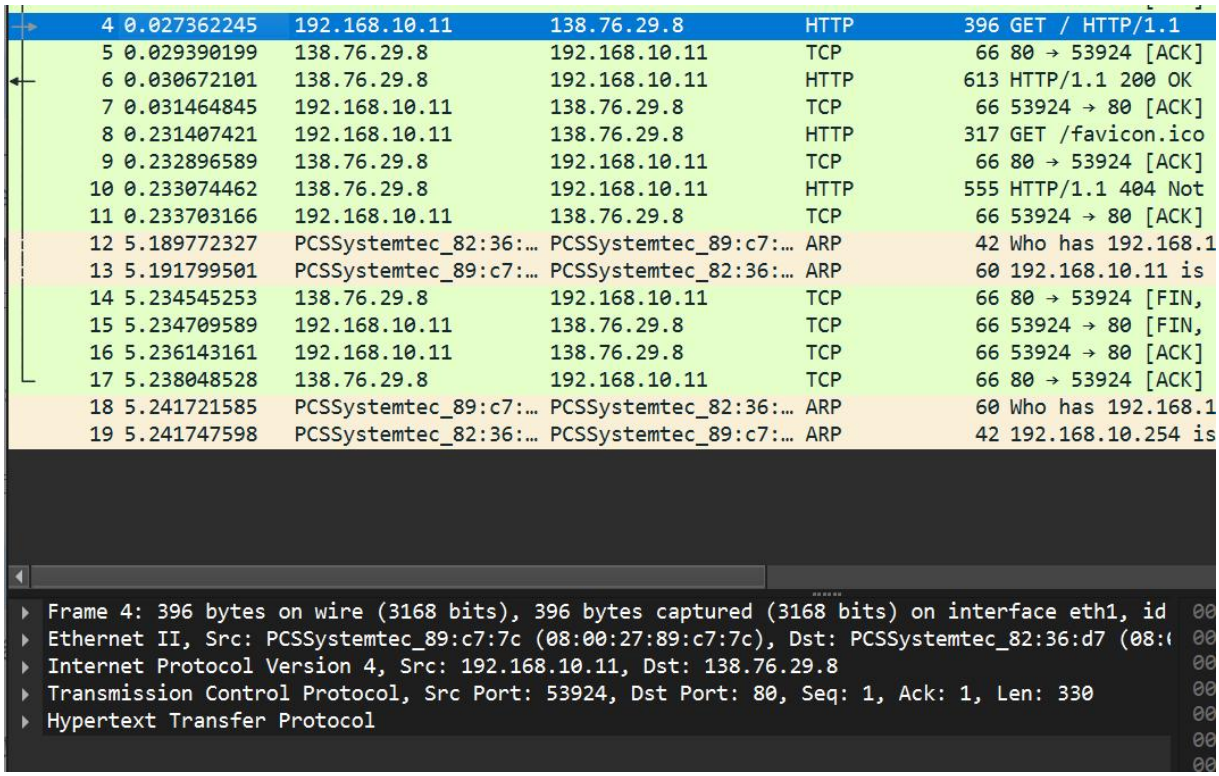
在下文中，我们将重点介绍这两条 HTTP 消息（GET 和 200 OK）。我们下面的目标是在跟踪文件 nat-outside-wireshark trace1-1.pcapng 中找到这两条 HTTP 消息，该文件是在路由器和 ISP 之间的 Internet 端链路上捕获的。由于捕获的发往服务器的数据包已通过 NAT 路由器转发，因此某些 IP 地址和端口号将因 NAT 转换而发生更改。打开跟踪文件

nat-outsid e-wireshark-trace1-1.pcapng 。请注意，此文件中的时间戳和 nat-inside-wireshark-trace1-1.pcapng 文件中的时间戳不一定同步。在 nat-outsid e-wireshark-trace1-1.pcapng 跟踪文件中，找到与在时间 t=0.27362245 从客户端发送到 138.76.29.8 服务器的 HTTP GET 消息相对应的 HTTP GET 消息，其中 t=0.27362245 是此消息的发送时间，如 nat-inside-wireshark-trace1-1.pcapng 跟踪文件中记录的那样。

让我们继续看一下 nat-outsid e-wireshark-trace1-1.pcapng 跟踪文件。找到包含“200 OK”消息的 HTTP 回复，该消息是针对您刚刚在上面的问题 4-8 中检查的 HTTP GETrequest 而收到的。

最后，让我们考虑一下，当 NAT 路由器收到在问题 9 和 10 中检查的此数据报，执行 NAT 转换，最后将该数据报转发到 LAN 端的目标主机时会发生什么情况。

1.在 nat inside-wireshark-trace1-1.pcapng 跟踪中发送 HTTP GET 请求的客户端的 IP 地址是什么？此包含 HTTP GET 请求的数据报中 TCPsegment 的源端口号是什么？什么是此 HTTP GET 请求的目标 IP 地址？此包含 HTTP GET 请求的数据报中 TCP 分段的目标端口号是什么？

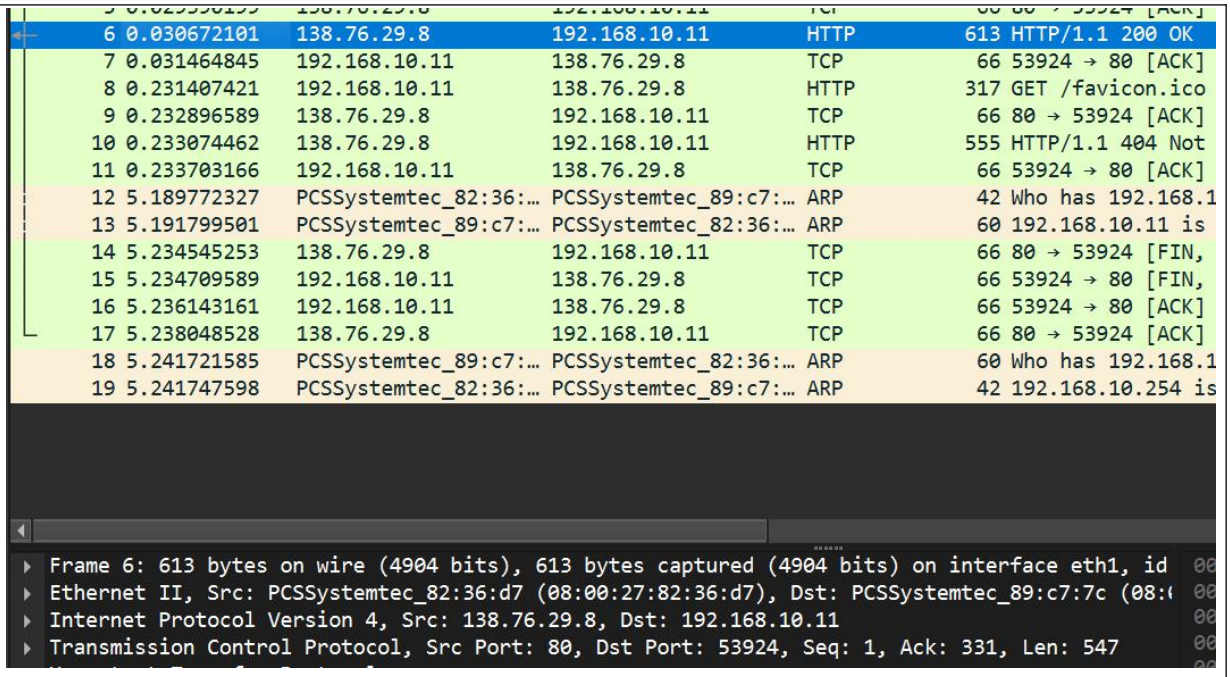


可以看到，客户端 ip 是 192.168.10.11，tcp 源端口是 53924；
目标 IP 地址是 138.76.29.8，tcp 目标端口是 80.

2.NAT 路由器在什么时间从 Web 服务器转发到路由器 LAN 端的客户端的相应 HTTP 200 OK 消息？

从上图“⬅”所在时间可以看到是 0.030672101 s。

3.携带此 HTTP 200 OK 消息的 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？

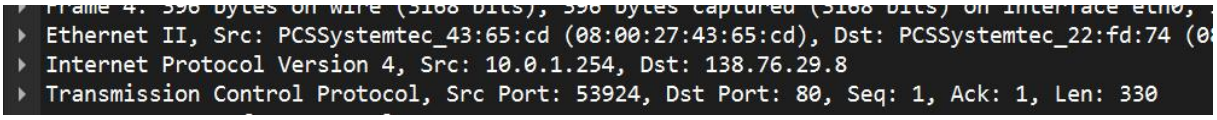


可以看到，源 ip 是 138.76.29.8，tcp 源端口是 80；
目标 IP 地址是 192.168.10.11，tcp 目标端口是 53924.

4.此 HTTP GET 消息何时出现在 nat-outside-wireshark trace1-1.pcapng 跟踪文件中？

是 0.027356291 s。

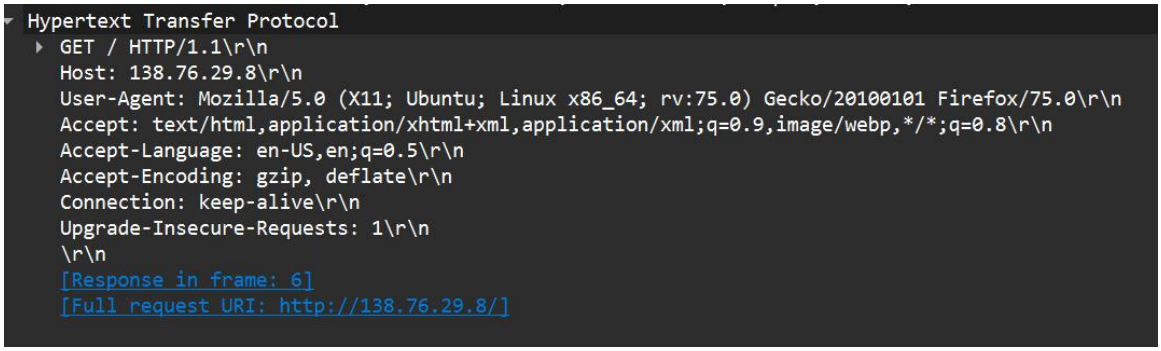
5.携带此 HTTP GET 的 IP 数据报上的源和目标 IP 地址以及 TCP 源和目标端口号是什么（如 nat outside-wireshark-trace1-1.pcapng 跟踪文件中记录的）？



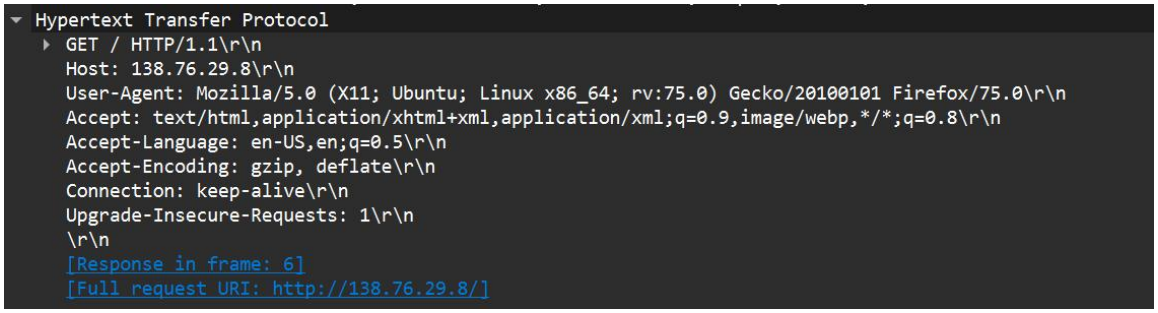
源 ip：10.0.1.254，目标 ip：138.76.29.8
源端口：53924，目标端口：80

6.这四个字段中的哪一个与您对上述问题 1 的回答不同？
源 IP

7. HTTP GET 消息中的任何字段是否更改？
Inside：



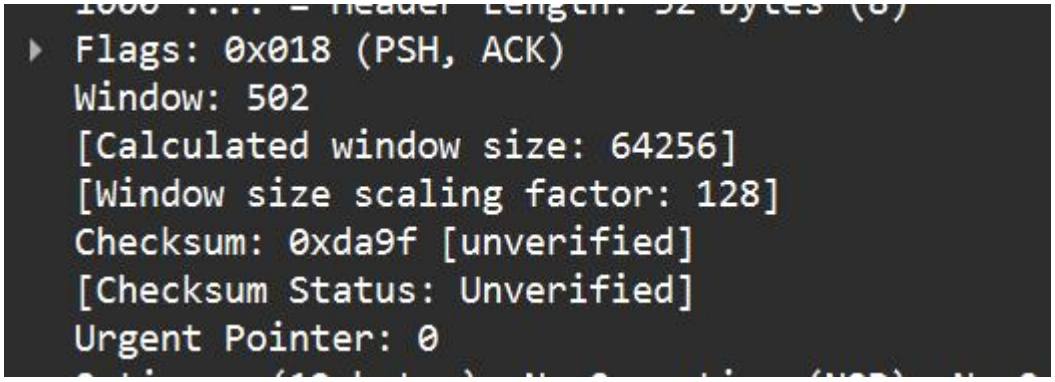
Outside：



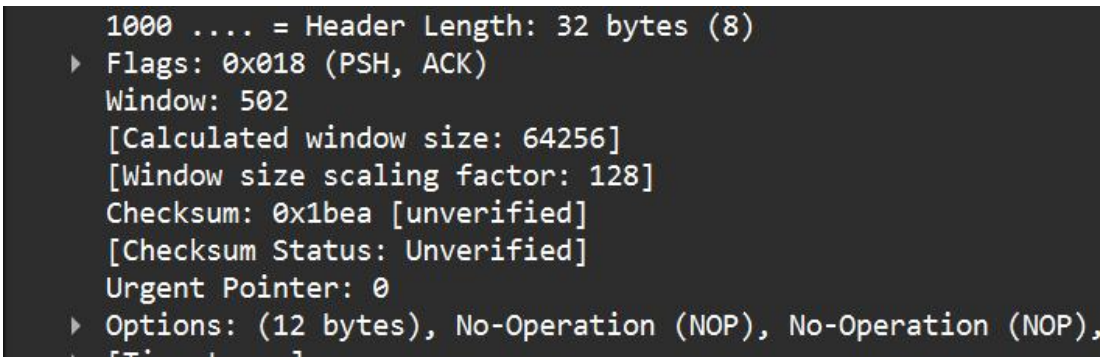
发现没有任何区别。

8. 携带 HTTP GET 的 IP 数据报中的以下哪些字段从局域网（内部）接收的数据报更改为在 NAT 路由器的 Internet 端（外部）转发的相应数据报：版本、报头长度、标志、校验和？

Outside：

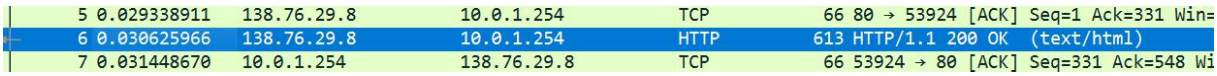


Inside：



发现 checksum 更改，而版本、报头长度、标志都没变。

9. 此消息何时出现在 nat-outside-wireshark-trace1 1.pcapng 跟踪文件中？



0.030625966 s。

10. 携带此 HTTP 回复（“200 OK”）消息的 IP 数据报上的源和目标 IP 地址以及 TCP 源和目标端口号是什么（如 nat-outside-wireshark-trace1-1.pcapng 跟踪文件中记录的）？

目标 ip：10.0.1.254， 源 ip：138.76.29.8

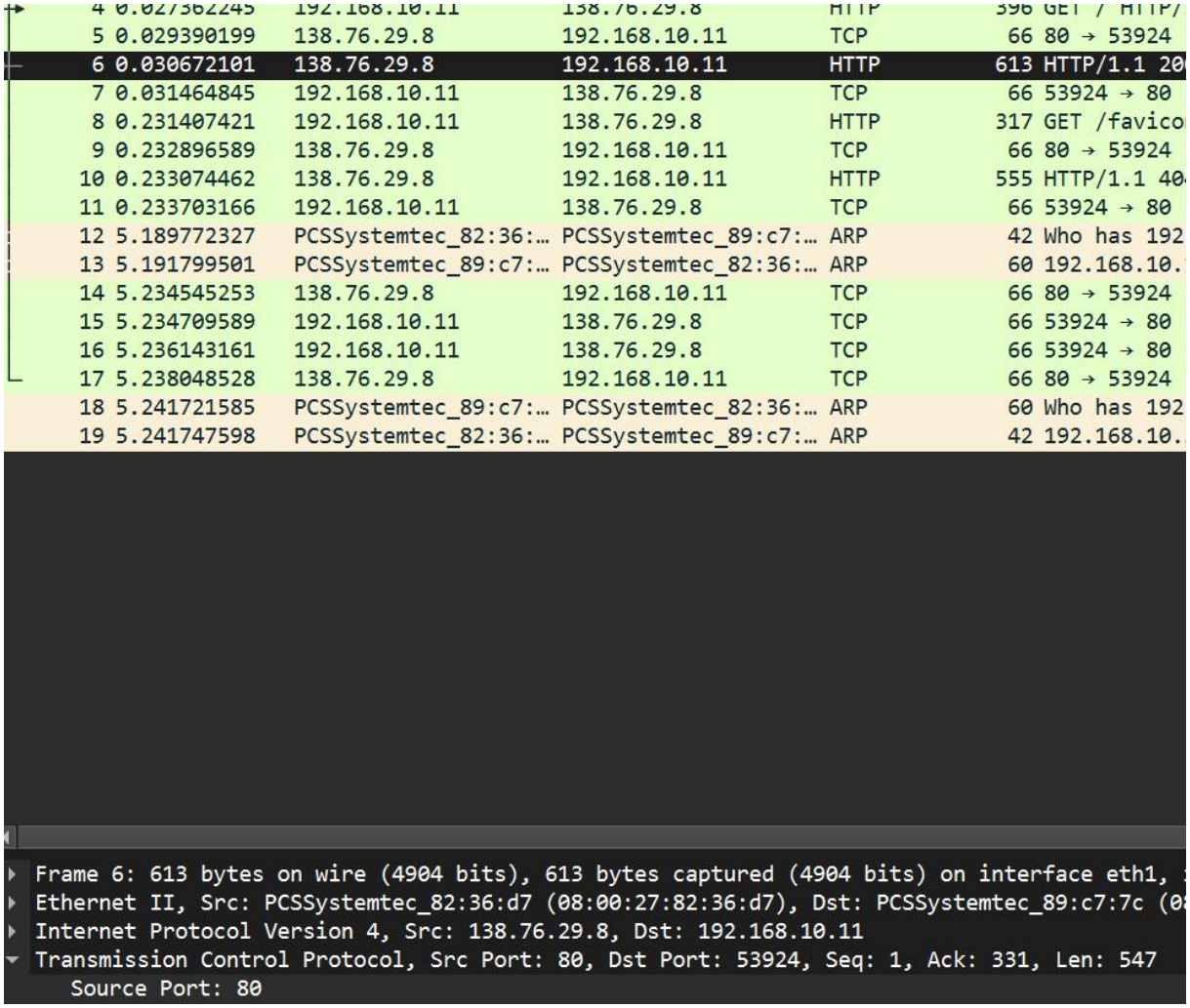
目标端口：53924，源端口：80

11. 图 1 右侧带有从路由器转发到目标主机的 HTTP 应答（“200 OK”）的 IP 数据报上的源和目标 IP 地址以及 TCP 源端口号和目标端口号是什么？

源 ip 是 138.76.29.8，tcp 源端口是 80；

目标 IP 地址是 192.168.10.11，tcp 目标端口是 53924.

与 inside 文件里面一样：



结论分析与体会：
通过此次实验我对 NAT 理解更进一步。