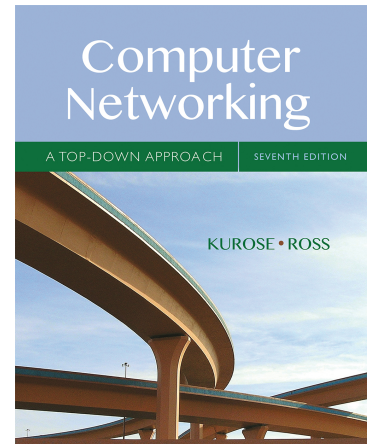


# Wireshark Lab: NAT v7.0

Supplement to *Computer Networking: A Top-Down Approach*, 7<sup>th</sup> ed., J.F. Kurose and K.W. Ross

“Tell me and I forget. Show me and I remember. Involve me and I understand.” Chinese proverb

© 2005-2012, J.F Kurose and K.W. Ross, All Rights Reserved



In this lab, we'll investigate the behavior of the NAT protocol. This lab will be different from our other Wireshark labs, where we've captured a trace file at a single Wireshark measurement point. Because we're interested in capturing packets at both the input and output sides of the NAT device, we'll need to capture packets at *two* locations. Also, because many students don't have easy access to a NAT device or to two computers on which to take Wireshark measurements, this isn't a lab that is easily done “live” by a student. Therefore in this lab, you will use Wireshark trace files that we've captured for you. Before beginning this lab, you'll probably want to review the material on NAT section 4.3.4 in the text<sup>1</sup>.

在本实验中，我们将研究 NAT 协议内容。本次实验不同于过去以往实验，我们将会在每个 Wireshark 捕获点抓包（译者注：在多个位置网络位置抓包，见下文）：我们将会在 NAT 设备出口和入口两个位置都要抓包。由于学生们可能没有轻松在 NAT 设备抓包的权限以及学生没有两台以上的电脑用以抓包，所以可能此实验不能由学生亲自完成，请使用作者提供的跟踪文件进行分析。另外，建议开始本实验之前，翻看课本中 4.3.4 节关于 NAT 内容。

## 1. NAT Measurement Scenario NAT 侦测场景

In this lab, we'll capture packets from a simple web request from a client PC in a home network to a [www.google.com](http://www.google.com) server. Within the home network, the home network router provides a NAT service, as discussed in Chapter 4. Figure 1 shows our Wireshark trace-collection scenario. As in our other Wireshark labs, we collect a Wireshark trace on the client PC in our home network. This file is called NAT\_home\_side<sup>2</sup>. Because we are

<sup>1</sup> References to figures and sections are for the 7<sup>th</sup> edition of our text, *Computer Networks, A Top-down Approach*, 7<sup>th</sup> ed., J.F. Kurose and K.W. Ross, Addison-Wesley/Pearson, 2016.

课本：计算机网络 自顶向下方方法第 7 版 中文版由机械工业出版社翻译发行

<sup>2</sup> Download the zip file <http://gaia.cs.umass.edu/wireshark-labs/wireshark-traces.zip> and extract the files need for this lab.

从 <http://gaia.cs.umass.edu/wireshark-labs/wireshark-traces.zip> 下载作者抓包结果，解压并打开它。

also interested in the packets being sent by the NAT router into the ISP, we'll collect a second trace file at a PC (not shown) tapping into the link from the home router into the ISP network, as shown in Figure 1. (The hub device shown on the ISP side of the router is used to tap into the link between the NAT router and the first hop router in the ISP). Client-to-server packets captured by Wireshark at this point will have undergone NAT translation. The Wireshark trace file captured on the ISP side of the home router is called NAT\_ISP\_side.

在本实验中，我们将会用在家庭网络的一个客户端 PC 发送到 [www.google.com](http://www.google.com) 简单 HTTP 请求并且捕获它。在家庭网络中，家庭网络路由器会提供如课本第四章所讲的 NAT 服务。图 1 显示我们的 Wireshark NAT 实验抓包收集方案。正如我们其它 Wireshark 实验一样，我们将会在该客户端 PC 进行抓包并保存为 NAT\_home\_side 文件。同样我们因为需要研究 NAT 路由器发送到 ISP 网络的数据包感兴趣，因此我们将会一个图 1 中的未展示 PC 收集从 NAT 路由到 ISP 网络的第二数据包。路由左侧连接 ISP 网络的集线器将会起到连接 NAT 路由器和 ISP 的第一跳路由（第一级路由的作用）。我们将位于 NAT 路由连 ISP 网络的 Wireshark 的抓包结果称为 NAT\_ISP\_side。

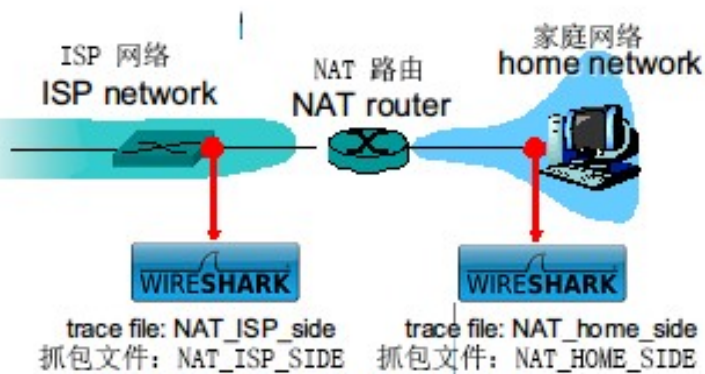


Figure 1: NAT trace collection scenario

图 1 NAT抓包收集方案

Open the NAT\_home\_side file and answer the following questions. You might find it useful to use a Wireshark filter so that only frames containing HTTP messages are displayed from the trace file.

打开 NAT\_home\_side 文件并回答以下问题。请使用 HTTP 过滤器过滤跟踪文件降低分析难度。

Whenever possible, when answering a question below, you should hand in a printout of the packet(s) within the trace that you used to answer the question asked. Annotate the printout<sup>3</sup> to explain your answer. To print a packet, use *File->Print*, choose *Selected*

<sup>3</sup> What do we mean by “annotate”? If you hand in a paper copy, please highlight where in the printout you’ve found the answer and add some text (preferably with a colored pen) noting what you found in what you’ve highlight. If you hand in an electronic copy, it would be great if you could also highlight and annotate.

请善用标记展示你的实验结果。

*packet only*, choose *Packet summary line*, and select the minimum amount of packet detail that you need to answer the question

请尽量清晰的展示您的答案，必要时您可以在图中用标记辅以说明。您的答案应该简单可读。

1. What is the IP address of the client?  
客户端的 IP 地址是多少？
2. The client actually communicates with several different Google servers in order to implement “safe browsing.” (See extra credit section at the end of this lab). The main Google server that will serve up the main Google web page has IP address 64.233.169.104. In order to display only those frames containing HTTP messages that are sent to/from this Google, server, enter the expression “http && ip.addr == 64.233.169.104” (without quotes) into the Filter: field in Wireshark .  
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”。（请参阅本实验结束的额外问题）。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式“ http && ip.addr == 64.233.169.104 ”（不包括引号）。
3. Consider now the HTTP GET sent from the client to the Google server (whose IP address is IP address 64.233.169.104) at time 7.109267. What are the source and destination IP addresses and TCP source and destination ports on the IP datagram carrying this HTTP GET?  
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 源和目标端口是什么？
4. At what time<sup>4</sup> is the corresponding 200 OK HTTP message received from the Google server? What are the source and destination IP addresses and TCP source and destination ports on the IP datagram carrying this HTTP 200 OK message?  
什么时候从 Google 服务器收到相应的状态码 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？
5. Recall that before a GET command can be sent to an HTTP server, TCP must first set up a connection using the three-way SYN/ACK handshake. At what time is the client-to-server TCP SYN segment sent that sets up the connection used by the GET sent at time 7.109267? What are the source and destination IP addresses and source and destination ports for the TCP SYN segment? What are the source and destination IP addresses and source and destination ports of the ACK sent in response to the SYN. At what time is this ACK received at the client? (Note: to find these segments you will need to clear the Filter expression you entered above in step 2. If you enter the filter “tcp”, only TCP segments will be displayed by Wireshark).

---

<sup>4</sup> Specify time using the time since the beginning of the trace (rather than absolute, wall-clock time).  
使用自跟踪开始以来的时间（而不是系统时间）指定时间。

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？为响应 SYN 报文而发送的 ACK 报文的源和目标 IP 地址以及源和目标端口是什么？在客户端收到此 ACK 报文什么时间？（注意您需要清除在第 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。

In the following we'll focus on the two HTTP messages (GET and 200 OK) and the TCP SYN and ACK segments identified above. Our goal below will be to locate these two HTTP messages and two TCP segments in the trace file (NAT\_ISP\_side) captured on the link between the router and the ISP. Because these captured frames will have already been forwarded through the NAT router, some of the IP address and port numbers will have been changed as a result of NAT translation.

在接下来实验中，我们将会重点关注 HTTP GET 和 HTTP 200 OK 消息以及刚才提到的 TCP SYN 报文和 TCP ACK 报文。我们的目标是在路由器和 ISP 之间的链路上捕获的跟踪文件 (NAT\_ISP\_side) 中找到这两个 HTTP 消息和两个 TCP 报文。由于这些捕获的帧已经通过 NAT 路由器转发，因此一些 IP 地址和端口号将因 NAT 转换而被更改。

Open the NAT\_ISP\_side. *Note that the time stamps in this file and in NAT\_home\_side are not synchronized since the packet captures at the two locations shown in Figure 1 were not started simultaneously.* (Indeed, you should discover that the timestamps of a packet captured at the ISP link is actually less than the timestamp of the packet captured at the client PC).

打开作者抓包文件 NAT\_ISP\_side。请注意此文件的时间戳不用于刚才的 NAT\_home\_side 的时间戳，因为两个位置捕获的信息并不是同步的。（实际上，您应该发现在 ISP 链路与 NAT 路由器的抓包时间戳小于在客户端 PC 上抓包的数据包的时间戳）

6. In the NAT\_ISP\_side trace file, find the HTTP GET message was sent from the client to the Google server at time 7.109267 (where t=7.109267 is time at which this was sent as recorded in the NAT\_home\_side trace file). At what time does this message appear in the NAT\_ISP\_side trace file? What are the source and destination IP addresses and TCP source and destination ports on the IP datagram carrying this HTTP GET (as recording in the NAT\_ISP\_side trace file)? Which of these fields are the same, and which are different, than in your answer to question 3 above?

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？与您对上述问题 3 的回答相比，哪些字段相同，哪些字段不同？

7. Are any fields in the HTTP GET message changed? Which of the following fields in the IP datagram carrying the HTTP GET are changed: Version, Header Length, Flags, Checksum. If any of these fields have changed, give a reason (in one sentence) stating why this field needed to change.  
HTTP GET 消息中的任何字段是否已更改? 携带 HTTP GET 的 IP 数据报中的以下哪个字段发生了变化: 版本, 标题长度, 标志, 校验和。如果这些字段中的任何一个发生了变化, 请说明为什么。
8. In the NAT\_ISP\_side trace file, at what time is the first 200 OK HTTP message received from the Google server? What are the source and destination IP addresses and TCP source and destination ports on the IP datagram carrying this HTTP 200 OK message? Which of these fields are the same, and which are different than your answer to question 4 above?  
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 数据报上的源和目标 IP 地址以及 TCP 源和目标端口是什么? 与您第 4 问回答的 NAT\_home\_side 结果相比哪些字段相同, 哪些字段不同?
9. In the NAT\_ISP\_side trace file, at what time were the client-to-server TCP SYN segment and the server-to-client TCP ACK segment corresponding to the segments in question 5 above captured? What are the source and destination IP addresses and source and destination ports for these two segments? Which of these fields are the same, and which are different than your answer to question 5 above?  
在 NAT\_ISP\_side 跟踪文件中, 跟上面的问题 5 相同地址的客户端到服务器 TCP SYN 报文和服务器到客户端 TCP ACK 报文在什么时间出现? 这两个段的源和目标 IP 地址以及源和目标端口是什么? 与您的问题 5 相比, 哪些字段相同, 哪些字段与不同?

Figure 4.25 in the text shows the NAT translation table in the NAT router.  
课本中的图 4.25 显示了 NAT 路由器中的 NAT 转换表。

10. Using your answers to 1-8 above, fill in the NAT translation table entries for HTTP connection considered in questions 1-8 above.  
使用您的第 1 到 8 题的答案, 做出跟课本类似的 HTTP 连接的 NAT 转换表。

**Extra Credit:** The trace files investigated above have additional connections to Google servers above and beyond the HTTP GET, 200 OK request/response studied above. For example, in the NAT\_home\_side trace file, consider the client-to-server GET at time 1.572315, and the GET at time 7.573305. Research the use of these two HTTP messages and write a half page explanation of the purpose of each of these messages.

额外问题: 在作者上面的抓包结果中, 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 1.572315 s 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 消息的使用并写出说明解释这些消息的目的。