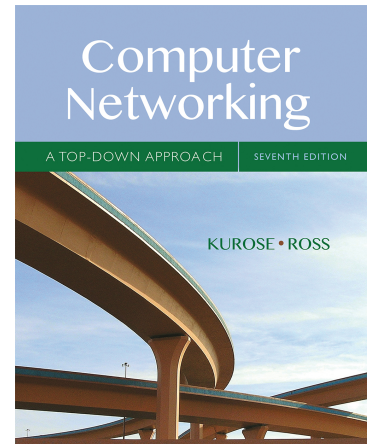


Wireshark Lab: UDP v7.0

Supplement to *Computer Networking: A Top-Down Approach*, 7th 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

© 2005-2016, J.F. Kurose and K.W. Ross, All Rights Reserved



In this lab, we'll take a quick look at the UDP transport protocol. As we saw in Chapter 3 of the text¹, UDP is a streamlined, no-frills protocol. You may want to re-read section 3.3 in the text before doing this lab. Because UDP is simple and sweet, we'll be able to cover it pretty quickly in this lab. So if you've another appointment to run off to in 30 minutes, no need to worry, as you should be able to finish this lab with ample time to spare.

在本实验中，我们将快速了解 UDP 传输协议。正如我们在本文第 3 章中所看到的，UDP 是一种简化的协议。在进行本实验之前，您可能需要重新阅读课本中的第 3.3 节。由于 UDP 简单易理解，您只需要一点花费时间就能做这个实验。

At this stage, you should be a Wireshark expert. Thus, we are not going to spell out the steps as explicitly as in earlier labs. In particular, we are not going to provide example screenshots for all the steps.

我们默认认同您已经熟悉 Wireshark 的操作，因此我们不会提供详细的截图说明和操作步骤。

The Assignment

Start capturing packets in Wireshark and then do something that will cause your host to send and receive several UDP packets. It's also likely that just by doing nothing (except capturing packets via Wireshark) that some UDP packets sent by others will appear in your trace. In particular, the Simple Network Management Protocol (SNMP – see section 5.7 in the text) sends SNMP messages inside of UDP, so it's likely that you'll find some SNMP messages (and therefore UDP packets) in your trace.

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

课本：计算机网络 自顶向下第 7th 版，（译者注）中文版由机械工业出版社翻译发行

开始在 Wireshark 中捕获数据包，然后执行一些会导致主机发送和接收多个 UDP 数据包的操作。您也可以什么也不做，仅执行 wireshark 捕获以便获取其他程序发给您的 UDP 数据包。有一种特殊情况：简单网络管理协议（SNMP - 请参阅课本中的第 5.7 节）在 UDP 内部发送 SNMP 消息，因此您可能会在跟踪中找到一些 SNMP 消息（以及 UDP 数据包）。

After stopping packet capture, set your packet filter so that Wireshark only displays the UDP packets sent and received at your host. Pick one of these UDP packets and expand the UDP fields in the details window. If you are unable to find UDP packets or are unable to run Wireshark on a live network connection, you can download a packet trace containing some UDP packets.²

停止数据包捕获后，设置数据包筛选器，以便 Wireshark 仅显示在主机上发送和接收的 UDP 数据包。选择其中一个 UDP 数据包并在详细信息窗口中展开 UDP 字段。如果您无法找到 UDP 数据包或无法在实时网络连接上运行 Wireshark，则可以下载包含某些 UDP 数据包的数据包跟踪。

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 printout³ to explain your answer. To print a packet, use *File->Print*, choose *Selected packet only*, choose *Packet summary line*, and select the minimum amount of packet detail that you need to answer the question.

如果可能的话建议您使用 wireshark 的文件->打印功能将您跟踪回答数据包最小详细结果打印出来，并且通过注释圈出。

1. Select *one* UDP packet from your trace. From this packet, determine how many fields there are in the UDP header. (You shouldn't look in the textbook! Answer these questions directly from what you observe in the packet trace.) Name these fields.

² Download the zip file <http://gaia.cs.umass.edu/wireshark-labs/wireshark-traces.zip> and extract the file http-ethereal-trace-5, which contains some UDP packets carrying SNMP messages. The traces in this zip file were collected by Wireshark running on one of the author's computers. Once you have downloaded the trace, you can load it into Wireshark and view the trace using the *File* pull down menu, choosing *Open*, and then selecting the http-ethereal-trace-5 trace file.

请去下载作者的实验结果 <http://gaia.cs.umass.edu/wireshark-labs/wireshark-traces.zip> 并且解压，打开 http-ethereal-trace-5，此结果包含有 SNMP 的消息的 UDP 数据包。

³ 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.

所谓注释，就是希望您可以圈出和突出展现您的结果，以便显示给我们，建议您提交电子版的答案。

- 1.从跟踪中选择一个 UDP 数据包。从此数据包中，确定 UDP 标头中有多少字段。（建议不要查看课本，直接根据您的数据包跟踪结果回答），并为这些字段命名。
2. By consulting the displayed information in Wireshark's packet content field for this packet, determine the length (in bytes) of each of the UDP header fields.

2.通过查询 Wireshark 的数据包内容字段中显示的信息，确定每个 UDP 报头字段的长度（以字节为单位）。
3. The value in the Length field is the length of what? (You can consult the text for this answer). Verify your claim with your captured UDP packet.

3.长度字段中的值指的是什么？（此问题您可以参考课本）。使用捕获的 UDP 数据包验证您的声明。
4. What is the maximum number of bytes that can be included in a UDP payload? (Hint: the answer to this question can be determined by your answer to 2. above)

4. UDP 有效负载中可包含的最大字节数是多少？（提示：这个问题的答案可以通过你对上述 2 的回答来确定）
5. What is the largest possible source port number? (Hint: see the hint in 4.)

5.最大可能的源端口号是多少？（提示：见 4 中的提示）
6. What is the protocol number for UDP? Give your answer in both hexadecimal and decimal notation. To answer this question, you'll need to look into the Protocol field of the IP datagram containing this UDP segment (see Figure 4.13 in the text, and the discussion of IP header fields).

UDP 的协议号是什么？以十六进制和十进制表示法给出答案。要回答这个问题，您需要查看包含此 UDP 段的 IP 数据报的 Protocol 字段（参见书中的图 4.13 和 IP 头字段的讨论）。
7. Examine a pair of UDP packets in which your host sends the first UDP packet and the second UDP packet is a reply to this first UDP packet. (Hint: for a second packet to be sent in response to a first packet, the sender of the first packet should be the destination of the second packet). Describe the relationship between the port numbers in the two packets.

7.观察发送 UDP 数据包后接收响应的 UDP 数据包，这是对发送的 UDP 数据包的回复，请描述两个数据包中端口号之间的关系。（提示：对于响应 UDP 目的地应该为发送 UDP 包的地址）