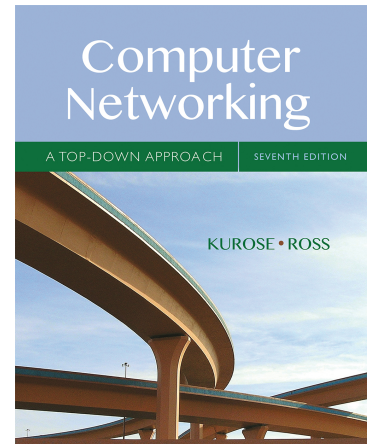


# Wireshark Lab: 802.11 v7.0

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

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



In this lab, we'll investigate the 802.11 wireless network protocol. Before beginning this lab, you might want to re-read Section 7.3 in the text<sup>1</sup>. Since we'll be delving a bit deeper into 802.11 than is covered in the text, you might want to check out “A Technical Tutorial on the 802.11 Protocol,” by Pablo Brenner (Breezecom Communications), [http://www.sss-mag.com/pdf/802\\_11tut.pdf](http://www.sss-mag.com/pdf/802_11tut.pdf), and “Understanding 802.11 Frame Types,” by Jim Geier, <http://www.wi-fiplanet.com/tutorials/article.php/1447501>. And, of course, there is the “bible” of 802.11 - the standard itself, “ANSI/IEEE Std 802.11, 1999 Edition (R2003),” <http://gaia.cs.umass.edu/wireshark-labs/802.11-1999.pdf>. In particular, you may find Table 1 on page 36 of the standard particularly useful when looking through the wireless trace.

在本实验中，我们将研究 802.11 无线协议。在开始本实验之前，建议您重新阅读课本的中第 7.3 节。因为我们将比课本深入研究 802.11 协议内容，因此您可能需要查看 Pablo Brenner (Breezecom Communications)写的《802.11 协议技术指南》(A Technical Tutorial on the 802.11 Protocol) ([http://www.sss-mag.com/pdf/802\\_11tut.pdf](http://www.sss-mag.com/pdf/802_11tut.pdf)) 以及 Jim Geier 写的《了解 802.11 帧类型》(Understanding 802.11 Frame Types) (<http://www.wi-fiplanet.com/tutorials/article.php/1447501>)。当然，您还需要查阅 802.11 的圣经-它的标准书《ANSI / IEEE 标准 802.11,1999 版 (R2003)》(ANSI/IEEE Std 802.11, 1999 Edition (R2003))(<http://gaia.cs.umass.edu/wireshark-labs/802.11-1999.pdf>)。您可能会发现标准书第 36 页的表 1 在分析无线跟踪特别有用。

In all of the Wireshark labs thus far, we've captured frames on a wired Ethernet connection. Here, since 802.11 is a wireless link-layer protocol, we'll be capturing frames “in the air.” Unfortunately, many device drivers for wireless 802.11 NICs don't provide the hooks to capture/copy received 802.11 frames for use in Wireshark (see Figure 1 in

<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

Lab 1 for an overview of packet capture). Thus, in this lab, we'll provide a trace of captured 802.11 frames for you to analyze and assume in the questions below that you are using this trace. If you're able to capture 802.11 frames using your version of Wireshark, you're welcome to do so. Additionally, if you're really into frame capture, you can buy a small USB device, AirPcap, <http://www.cacotech.com>, that captures 802.11 frames and provides integrated support for Wireshark.

在除本次实验以外其它的 Wireshark 实验中，我们都是在有线以太网连接进行抓包（捕获帧）。在本实验中，因为 802.11 是无线链路层协议，我们将在“空中”捕获帧。不幸的是，带有 802.11 协议的无线网卡（NIC）设备驱动无法提供钩子将捕获/接收的 802.11 帧用于 Wireshark 实验分析。因此，在本实验中，您可能会使用作者捕获的 802.11 帧（抓包结果）进行分析。如果您有能力自己捕获，欢迎您自己动手。如果您乐意自己跟踪，或许你可以买一个小的 USB 网卡 AirPcap 用以捕获 802.11 帧（[www.cacotech.com](http://www.cacotech.com)）。

## 1. Getting Started 开始实验

Download the zip file <http://gaia.cs.umass.edu/wireshark-labs/wireshark-traces.zip> and extract the file Wireshark\_802\_11.pcap. This trace was collected using AirPcap and Wireshark running on a computer in the home network of one of the authors, consisting of a Linksys 802.11g combined access point/router, with two wired PCs and one wireless host PC attached to the access point/router. The author is fortunate to have other access points in neighboring houses available as well. In this trace file, we'll see frames captured on channel 6. Since the host and AP that we are interested in are not the only devices using channel 6, we'll see a lot of frames that we're not interested in for this lab, such as beacon frames advertised by a neighbor's AP also operating on channel 6. The wireless host activities taken in the trace file are:

从 <http://gaia.cs.umass.edu/wireshark-labs/wireshark-traces.zip> 下载压缩包并且得到 Wireshark\_802\_11.pcap。本结果由团队的一个作者在家庭网络使用 AirPcap 以及运行 Wireshark 的计算机得到，结果其中包括 Linksys 802.11g 的组合接入点（路由器），该接入点为两台有线 PC 和一台无线 PC 提供服务。作者幸运邻居也使用无线接入点。在此跟踪文件中，我们能看到在通道 6 上捕获的帧。由于我们需要分析主机和接入点不是使用通道 6 的唯一组合，我们也会看到其他例如邻居接入点使用通道 6 被作者收集到。跟踪文件中采用的无线主机活动包括：

- The host is already associated with the *30 Munroe St* AP when the trace begins. 跟踪开始时，主机已经与 *30 Munroe St* 接入点关联（associated）。
- At  $t = 24.82$ , the host makes an HTTP request to <http://gaia.cs.umass.edu/wireshark-labs/alice.txt>. The IP address of [gaia.cs.umass.edu](http://gaia.cs.umass.edu) is 128.119.245.12.  
在时间 24.82 时刻，主机向 IP 地址 128.119.245.12 的服务器发送 HTTP 请求，请求内容是 <http://gaia.cs.umass.edu/wireshark-labs/alice.txt>。
- At  $t=32.82$ , the host makes an HTTP request to <http://www.cs.umass.edu>, whose IP address is 128.119.240.19.

在时间 32.82 时刻，主机向 IP 地址 128.119.240.19 的服务器发送 HTTP 请求，请求内容是 <http://www.cs.umass.edu>。

- At  $t = 49.58$ , the host disconnects from the *30 Munroe St* AP and attempts to connect to the *linksys\_ses\_24086*. This is not an open access point, and so the host is eventually unable to connect to this AP.  
在时间 49.58 的时刻，主机断开了与 *30 Munroe St* 接入点的关联，并且尝试连接到 *linksys\_ses\_24086* 接入点。该接入点不是开放的接入点，因此主机始终没有成功与该接入点关联成功。
- At  $t=63.0$  the host gives up trying to associate with the *linksys\_ses\_24086* AP, and associates again with the *30 Munroe St* access point.  
在时间 63.0 时刻，主机放弃尝试关联 *linksys\_ses\_24086* 接入点，并且再次连接 *30 Munroe St* 接入点关联。

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 Wireshark\_802\_11.pcap trace file. The resulting display should look just like Figure 1. 下载作者的抓包结果后，使用 Wireshark 的 File 菜单打开该文件 Wireshark\_802\_11.pcap，您应该看到与图 1 显示相同的结果。

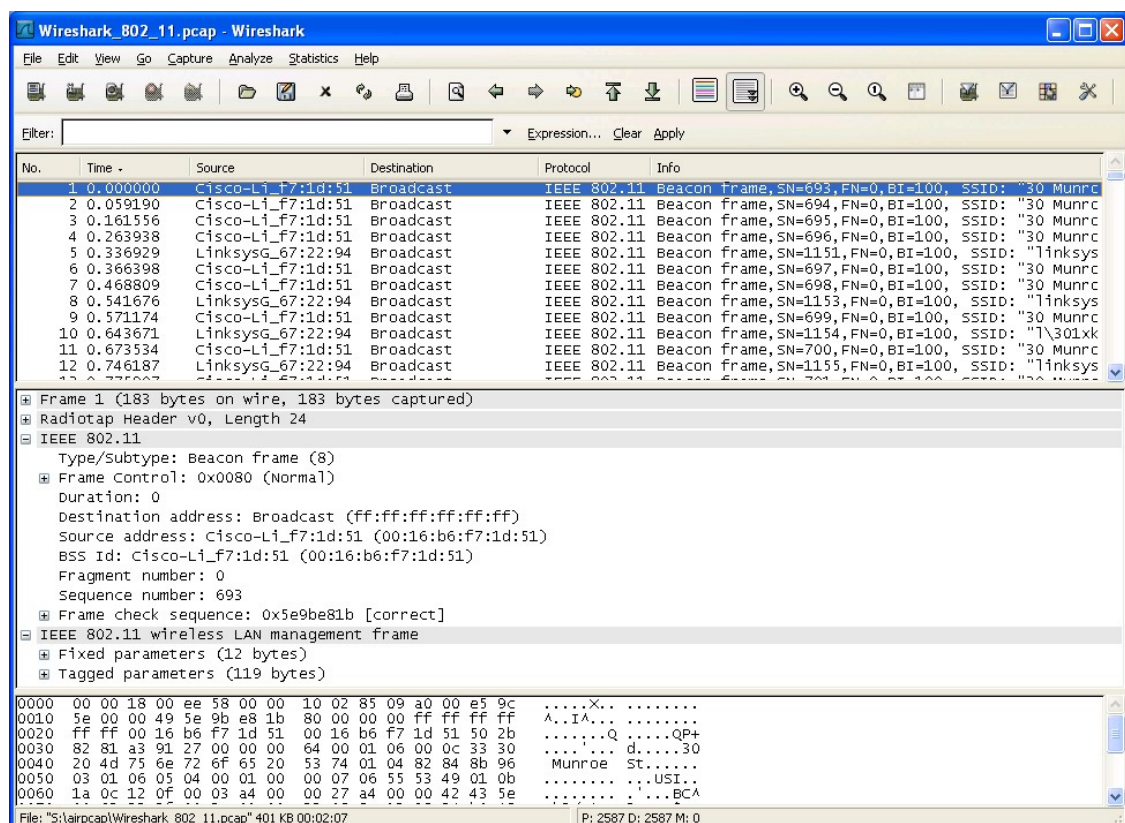


Figure 1: Wireshark window, after opening the Wireshark\_802\_11.pcap file

图 1: 打开 Wireshark\_802\_11.pcap 文件后的 Wireshark 窗口

## 2. Beacon Frames 信标帧

Recall that beacon frames are used by an 802.11 AP to advertise its existence. To answer some of the questions below, you'll want to look at the details of the "IEEE 802.11" frame and subfields in the middle Wireshark window. 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>2</sup> 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.

回想一下，802.11 接入点使用信标帧表示其存在。要回答下面的问题，您或许应该展开 IEEE 802.11 帧并在 Wireshark 中间窗口看到它的字段详细信息。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 are the SSIDs of the two access points that are issuing most of the beacon frames in this trace?  
发送最多信标帧的两个接入点的服务集标识符是多少 (SSID) ?
2. What are the intervals of time between the transmissions of the beacon frames the *linksys\_ses\_24086* access point? From the *30 Munroe St.* access point? (Hint: this interval of time is contained in the beacon frame itself).  
*linksys\_ses\_24086* 接入点和 *30 Munroe St.*接入点的信标帧传输时间是多少?  
(提示：此时间间隔包含在信标帧本身之中。)
3. What (in hexadecimal notation) is the source MAC address on the beacon frame from *30 Munroe St*? Recall from Figure 7.13 in the text that the source, destination, and BSS are three addresses used in an 802.11 frame. For a detailed discussion of the 802.11 frame structure, see section 7 in the IEEE 802.11 standards document (cited above).  
请以十六进制表示法找到 *30 Munroe St* 接入点的源 MAC 地址。回想课本中图 7-13，并说明源地址，目的地址，基本服务集 (BSS) 的地址是什么。有关 802.11 帧结构的详细讨论说明，请参阅 IEEE 802.11 标准文档（上文所提）中的第 7 节。
4. What (in hexadecimal notation) is the destination MAC address on the beacon frame from *30 Munroe St*?  
*30 Munroe St* 接入点的信标帧目的地址十六进制表示是什么？
5. What (in hexadecimal notation) is the MAC BSS id on the beacon frame from *30 Munroe St*?  
*30 Munroe St* 接入点的 BSS ID 地址是什么？

---

<sup>2</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。

6. The beacon frames from the *30 Munroe St* access point advertise that the access point can support four data rates and eight additional “extended supported rates.” What are these rates?

来自 *30 Munroe St* 接入点的信标帧宣告接入点可以支持四种数据速率和八种额外的“扩展支持速率”。这些速率是多少？

### 3. Data Transfer 数据传输

Since the trace starts with the host already associated with the AP, let first look at data transfer over an 802.11 association before looking at AP association/disassociation.

Recall that in this trace, at  $t = 24.82$ , the host makes an HTTP request to <http://gaia.cs.umass.edu/wireshark-labs/alice.txt>. The IP address of [gaia.cs.umass.edu](http://gaia.cs.umass.edu) is 128.119.245.12. Then, at  $t=32.82$ , the host makes an HTTP request to <http://www.cs.umass.edu>.

由于作者抓包开始时，主机已经与 AP 关联，因此在做下面 AP 关联/解除关联之前，我们首先研究已经主机与关联 802.11 AP 的数据传输。回想一下，在作者抓包结果中，在时间 24.82 的时刻，主机向 <http://gaia.cs.umass.edu/wireshark-labs/alice.txt> 发出 HTTP 请求。[gaia.cs.umass.edu](http://gaia.cs.umass.edu) 的 IP 地址是 128.119.245.12。然后，在 32.82 时刻，主机向 <http://www.cs.umass.edu> 发出 HTTP 请求。

7. Find the 802.11 frame containing the SYN TCP segment for this first TCP session (that downloads *alice.txt*). What are three MAC address fields in the 802.11 frame? Which MAC address in this frame corresponds to the wireless host (give the hexadecimal representation of the MAC address for the host)? To the access point? To the first-hop router? What is the IP address of the wireless host sending this TCP segment? What is the destination IP address? Does this destination IP address correspond to the host, access point, first-hop router, or some other network-attached device? Explain.

找到包含第一个 TCP SYN TCP 报文（下载 *alice.txt* 会话）的 802.11 帧。

802.11 帧中三个 MAC 地址字段分别是什么？此帧中那个 MAC 地址对应十六进制的无线主机的 MAC 地址？那个对应接入点 MAC 地址，第一跳路由器的 MAC 地址？发送此 TCP 报文的无线主机 IP 是什么？目的地 IP 地址是什么？此目的地是否与主机地址，接入点地址，第一跳路由器地址或者某些其他网络设备相对应，解释并且说明。

8. Find the 802.11 frame containing the SYNACK segment for this TCP session. What are three MAC address fields in the 802.11 frame? Which MAC address in this frame corresponds to the host? To the access point? To the first-hop router? Does the sender MAC address in the frame correspond to the IP address of the device that sent the TCP segment encapsulated within this datagram? (Hint: review Figure 6.19 in the text if you are unsure of how to answer this question, or the corresponding part of the previous question. It's particularly important that you understand this).

找到包含此 TCP 会话 SYN ACK 报文的 802.11 帧。该帧中三个 MAC 地址字段是什么？那个 MAC 地址对应十六进制的无线主机的 MAC 地址？那个对应接入点 MAC 地址，第一跳路由器的 MAC 地址？帧中的发送方 MAC 地址是否与发送此 TCP 报文的设备的 IP 地址相对应？

### 3. Association/Disassociation 关联/解除关联

Recall from Section 7.3.1 in the text that a host must first *associate* with an access point before sending data. Association in 802.11 is performed using the ASSOCIATE REQUEST frame (sent from host to AP, with a frame type 0 and subtype 0, see Section 7.3.3 in the text) and the ASSOCIATE RESPONSE frame (sent by the AP to a host with a frame type 0 and subtype of 1, in response to a received ASSOCIATE REQUEST). For a detailed explanation of each field in the 802.11 frame, see page 34 (Section 7) of the 802.11 spec at <http://gaia.cs.umass.edu/wireshark-labs/802.11-1999.pdf>.

回想一下课本的第 7.3.1 节，主机在发送数据之前必须与接入点关联。802.11 中的关联使用 ASSOCIATE REQUEST 帧（从主机发送到 AP，帧类型 0 和子类型 0，参见本文中的第 7.3.3 节）和 ASSOCIATE RESPONSE 帧（由 AP 发送给具有主机，帧类型 0 和子类型 1，响应于接收到的 ASSOCIATE REQUEST）。有关 802.11 帧中每个字段的详细说明，请参阅 <http://gaia.cs.umass.edu/wireshark-labs/802.11-1999.pdf> 中 802.11 规范的第 34 页（第 7 节）。

9. What two actions are taken (i.e., frames are sent) by the host in the trace just after  $t=49$ , to end the association with the *30 Munroe St* AP that was initially in place when trace collection began? (Hint: one is an IP-layer action, and one is an 802.11-layer action). Looking at the 802.11 specification, is there another frame that you might have expected to see, but don't see here?

在时间 49 的时刻，主机在跟踪中使用那两个动作（例如：发送帧）解除在跟踪开始之前就已经连接的 *30 Munroe St* AP 的关联。（提示：一个是 IP 层多宗，一个是 802.11 层动作）。在查看 802.11 规范之后，请找出抓包结果中未显示一个动作帧。

10. Examine the trace file and look for AUTHENTICATION frames sent from the host to an AP and vice versa. How many AUTHENTICATION messages are sent from the wireless host to the *linksys\_ses\_24086* AP (which has a MAC address of Cisco\_Li\_f5:ba:bb) starting at around  $t=49$ ?

在抓包结果中，找到主机发送给无线 AP 的 AUTHENTICATION 帧，同时也找无线 AP 的回复响应帧。在时间 49 时刻之后，无线主机向 *linksys\_ses\_24086* AP (MAC 地址包括 Cisco\_Li\_f5:ba:bb) 发送了多少 AUTHENTICATION 消息？

11. Does the host want the authentication to require a key or be open?

主机是否希望身份认证和关联 AP？

12. Do you see a reply AUTHENTICATION from the *linksys\_ses\_24086* AP in the trace?

您是否在跟踪中看到来自 *linksys\_ses\_24086* AP 回的 AUTHENTICATION？



13. Now let's consider what happens as the host gives up trying to associate with the *linksys\_ses\_24086* AP and now tries to associate with the *30 Munroe St* AP. Look for AUTHENTICATION frames sent from the host to and AP and vice versa. At what times are there an AUTHENTICATION frame from the host to the *30 Munroe St* AP, and when is there a reply AUTHENTICATION sent from that AP to the host in reply? (Note that you can use the filter expression "wlan.fc.subtype == 11 and wlan.fc.type == 0 and wlan.addr == IntelCor\_d1:b6:4f" to display only the AUTHENTICATION frames in this trace for this wireless host.)

现在让我们来分析当主机放弃尝试与 *linksys\_ses\_24086* AP 关联并且现在尝试与 *30 Munroe St* AP 关联发生什么。查找从主机发送到 AP 的 AUTHENTICATION 帧，同时也找无线 AP 的回复响应帧。在什么时间有一个主机到 *30 Munroe St* AP 的帧，在什么时间无线 AP 回主机该帧的回复。

(注意：您可以使用 "wlan.fc.subtype == 11 and wlan.fc.type == 0 and wlan.addr == IntelCor\_d1:b6:4f" (不含引号) 在此跟踪中仅显示无线主机的 AUTHENTICATION 帧)

14. An ASSOCIATE REQUEST from host to AP, and a corresponding ASSOCIATE RESPONSE frame from AP to host are used for the host to associated with an AP. At what time is there an ASSOCIATE REQUEST from host to the *30 Munroe St* AP? When is the corresponding ASSOCIATE REPLY sent? (Note that you can use the filter expression "wlan.fc.subtype < 2 and wlan.fc.type == 0 and wlan.addr == IntelCor\_d1:b6:4f" to display only the ASSOCIATE REQUEST and ASSOCIATE RESPONSE frames for this trace.)

从主机到 AP 的关联请求，以及相应的 AP 对主机关联请求的响应。在什么时候有来自主机到 AP 关联请求，什么时候 AP 对主机关联请求响应。(注意：你可以使用过滤表达式 "wlan.fc.subtype < 2 and wlan.fc.type == 0 and wlan.addr == IntelCor\_d1:b6:4f" 来仅显示 ASSOCIATE REQUEST 和 ASSOCIATE RESPONSE 帧。

15. What transmission rates is the host willing to use? The AP? To answer this question, you will need to look into the parameters fields of the 802.11 wireless LAN management frame.

主机和 AP 愿意使用什么传输速率？要回答此问题，您或许要查看 802.11 无线管理帧的字段。

#### 4. Other Frame types 其他帧类型

Our trace contains a number of PROBE REQUEST and PROBE RESPONSE frames. 作者的抓包结果中含许多 PROBE REQUEST 和 PROBE RESPONSE 帧。

16. What are the sender, receiver and BSS ID MAC addresses in these frames? What is the purpose of these two types of frames? (To answer this last question, you'll need to dig into the online references cited earlier in this lab).

这些帧中的发送方，接收方和 BSS ID MAC 地址是什么？这两种帧的目的是什么？(要回答最后一个问题，您需要深入研究本实验前面引用说明的在线参考资料)。