|  |  |  |  |
| --- | --- | --- | --- |
| **《计算机网络》实验报告** | | | |
| **实验编号** | 实验三 | **实验名称** | 802.11 |
| **姓名** | 叶俊 | **学号** | 202200201151 |
| **班级** | 菁英班 | **成绩** |  |
| 1. **实验目的**   了解802.11的物理层、链路层和管理功能。 | | | |
| 1. **实验要求**   Wireshark:本实验使用Wireshark软件工具捕获和检测数据包的踪迹。 | | | |
| 1. **实验内容** 2. Capture a Trace 3. Inspect the Trace 4. 802.11 Physical Layer 5. 802.11 Link Layer 6. 802.11 Management | | | |
| 1. **实验过程** 2. 第一步 Capture a Trace 捕获追踪   因为我们不具备捕获802.11帧的能力，所以直接下载官方提供的包     1. 第二步 Inspect the Trace检查跟踪   选择一个数据包进行分析，这里选择了Beacon帧。    包括以下信息：   1. Frame记录：由wireshark添加的记录，是一个包装器，包含有关于原始数据帧的元数据，如捕获时间和帧长度。它包含了这些信息用于分析但不包含在无线网络实际传输的数据中。      1. Radiotap header：Radiotap头也是Wireshark或其他数据包嗅探工具添加的记录，用于提供底层无线网络的物理层信息，例如信噪比、信道、速率等。      1. 802.11 radio information：通过header（物理层信息）解析出来的信息。显示的与信号强度相关的信息。例如信噪比、信道、速率等。      1. IEEE 802.11数据帧：IEEE 802.11数据帧是在无线局域网（WLAN）中传输数据的基本单位。它定义了在IEEE 802.11标准下，无线设备之间如何封装和传输数据。一个IEEE 802.11数据帧通常包含以下几个主要部分：   展开Data帧的IEEE 802.11记录，详细信息如下：   1. 帧类型和子类型：指明这是一个信标帧。 2. 帧控制字段：提供关于帧的版本、类型和子类型的信息。例如，数据，以及各种标志。      1. 持续时间：告诉计算机在无线介质上需要多少时间来处理作为交换一部分的附加数据包。 2. 接收者和发送者地址：标识数据包的目的地和来源。 3. BSS Id：基本服务集的标识符，通常是发送信标帧的无线接入点的MAC地址。 4. 序列号：数据包的序列号，用于数据包排序和控制。 5. 帧校验序列：用于检测数据包在传输过程中是否出现错误。      1. 第三步: 802.11 Physical Layer 802.11物理层   ****问题1:**** What is the channel frequency? To find the frequency, expand the Radiotap header of any frame and look for the Channel frequency.  如图：    信道频率：2437  为观察信噪比，添加数据速率和RSSI两个新的显示列，    结果如下    ****问题2：**** What rates are used? Give an ordered list of rates from lowest to highest. Hint: you can click the Rate column to sort by that value.  Rate：1.0，6.0，12.0，18.0, 24.0, 36.0, 48.0, 54.0  ****问题3：**** What is the range of RSSI and hence variation in SNRs in the trace? Give this as the strongest and weakest RSSI and the dB difference between them.  RSSI: 无线设备接收信号的功率电平的度量。这里RSSI的变化范围为-94~-21dBm  SNR（信噪比）变化范围为6~79dB，差值为73   1. 第四步：802.11 Link Layer(802.11链路层）   在统计——会话中，在协议中勾选IEEE 802.11，即可看到下图。    ****问题1：**** What is the BSS ID used by the most active wireless conversations? A BSS ID value identifies an AP, so this BSS ID identifies the most active AP, presumably the AP we are monitoring. To help find it, you can sort on the source or destination address by clicking on the column heading. We can also look to see the amounts we have of different types of traffic. 802.11 frames are either Data, Control, or Management frames. These frames are distinguished by the value in the Type subfield of the Frame Control field. You can inspect different packets to see the values for different types of frames.     1. 如图所示，最活跃的BSSID：00:16:b6:f7:1d:51   ****问题2：**** How many Data frames are in the trace, and what is the most common subtype of Data frame?   1. 共有777个数据帧，最常见的子类型是：0     ****问题3：**** How many Control frames are in the trace, and what is the most common subtype?   1. 共有616个控制帧，最常见的为13     ****问题4：**** How many Management frames are in the trace, and what is the most common subtype?   1. 共有960个management frame，最常见的为8，见下图     ****问题5：**** List in the order they are sent the IEEE 802.11 fields in an Acknowledgement frame and their lengths in bytes. Do not break down the Frame Control field into subfields, as we have already looked at these details.   1. 如图所示：     ****问题6：**** Give an estimate of the retransmission rate as the number of retransmissions over the number of original transmissions. Show your calculation.   1. 原始数据帧数量527，重传数据帧250，重传率250/527=0.474     ****问题7：****What fraction of the frames sent to the AP signal that the client is powering down?   1. 关机的用户：119，如图        1. Step5: 802.11 Management （802.11管理）   ****问题1：**** What is the SSID of the main AP? This is one of the tagged parameters in the Beacon frame.    ****问题2：**** How often are Beacon frames sent for the main AP? You may find the Beacon interval given in the Beacon frame itself, or change the Time display to be show the interval since the last frame. (Under View, select Time Display Format, and “Seconds Since Previous Displayed Packet”.)    ****问题3：**** What data rates does the main AP support? The rates are listed under tagged parameters.  支持数据速率6,9,12,18,24,36,48,54    **问题4：** What rate is the Beacon frame transmission? The answer to this question will be found on the Radiotap header, or more conveniently displayed in the column you added in an earlier step.  1.0Mb/s    ****问题5：**** What are the Type and Subtype values of Association Request / Association Response frames?  类型均为0，子类型Association request为0， Association response为1      ****问题6：**** What are the Type and Subtype values for the Probe Request / Probe Response frames?  类型均为0，子类型Probe request为4， Probe response为5  探测请求帧：    探测响应帧： | | | |
| **四．实验心得**  本次实验深入探讨了IEEE 802.11无线网络的关键层面，包括物理层、链路层以及管理功能。通过对帧结构的细致解析，我们深入了解了数据帧传输的具体机制，尤其是接收信号强度指示（RSSI）和信噪比（SNR）对网络性能的重要影响。在链路层的学习过程中，我们对网络会话的建立和维护有了更加深刻的认识。利用Wireshark工具，我们对数据帧、控制帧和管理帧等不同类型的帧进行了详尽的分析。  在管理功能实验部分，我们揭示了无线网络的组织结构以及设备如何加入和退出网络的整个过程。信标帧、关联请求帧和探测帧等管理帧的详细分析，展示了无线网络的逻辑结构和协议运作。通过本次实验，我们不仅掌握了无线网络的基本原理，也为未来的网络优化和故障排查打下了坚实的基础。 | | | |