山东大学 计算机 学院

计算机网络 课程实验报告

|  |  |  |  |
| --- | --- | --- | --- |
| 学号：202000130143 | 姓名： 郑凯饶 | | 班级： 2020级1班 |
| 实验题目：802.11 WiFi | | | |
| 实验学时：2 | | 实验日期： 2022-5-31 | |
| 实验目的：  研究802.11 WiFi协议 | | | |
| 硬件环境：  Dell Latitude 5411  Intel(R) Core(TM) i5-10400H CPU @ 2.60GHz(8GPUs),~2.6GHz | | | |
| 软件环境：  Windows 10 家庭中文版64位（10.0，版本18363）  Wireshark-win64-3.6.2 | | | |
| 实验步骤与内容：   1. 问题： 2. 发送最多信标帧的两个接入点的SSID？ 3. 24086和30 Munroe St.接入点的信标帧传输间隔是多少？ 4. 30 Munroe St.接入点的MAC地址。说明源地址、目的地址、BSS的地址是什么？ 5. 30 Munroe St.接入点的信标帧目的地址的16进制表示？ 6. 30 Munroe St.接入点的BSS ID地址？ 7. 30 Munroe St.接入点的信标帧宣告接入点可以支持4种数据速率和8种额外的“扩展支持速率”，这些速率是多少？   （7） 找到包含第1个TCP SYN TCP报文（下载alice.txt）的802.11帧。帧中3个MAC地址是什么？说明和无线主机、接入点、第1跳路由的对应关系？发送此TCP报文的无线主机IP是什么？目的IP是什么？解释他们之间的对应关系？  （8） 找到包含此TCP会话SYN ACK报文的802.11帧。回答问题类同（7）。  （9） 49时刻在跟踪中使用哪2个方法解除在跟踪之前与30 Munroe St.建立的关联？  （10） 找到主机发送给AP的AUTHENICATION帧，同时找到无线AP的回复响应帧。49时刻之后无线主机向24086发送了多少AUTHENICATION消息？  （11） 主机认证是希望通过key还是be open？  （12） 是否在跟踪中看到来自24086 AP回复AUTHENICATION？  （13） 分析主机放弃与24086 AP的关联并且尝试与30 Munroe St. AP关联的过程。查找从诸暨发送到AP的AUTHENICATION帧以及无线AP的回复响应帧。  （14） 主机到AP的关联请求以及AP到主机的请求响应被用于主机和AP之间的关联。查找关联的请求以及响应。  （15）主机愿意使用什么传输速率？  （16）回答PROBE REQUEST帧和PROBE RESPONSE帧的3个MAC地址，并解释这些帧的作用是什么？   1. 阐述基本方法              1. 实验结果展示与分析   （1）30 Munroe St和linksys12    （2）均为Beacon Interval: 0.102400 [Seconds]  （3）Source address: Cisco-Li\_f7:1d:51 (00:16:b6:f7:1d:51)  源地址是发送无线信号站点本身的地址，目的地址是接收无线信号站点的地址，基本服务集地址是指基本服务集基础设施的地址（AP的地址）。    （4）Destination address: Broadcast (ff:ff:ff:ff:ff:ff)表示广播地址  （5）BSS Id: Cisco-Li\_f7:1d:51 (00:16:b6:f7:1d:51)  （6）如下图       1. 接收、发送、目的MAC地址如下图所示。   无线主机MAC地址：Source address: IntelCor\_d1:b6:4f (00:13:02:d1:b6:4f)  接入点MAC地址：BSS Id: Cisco-Li\_f7:1d:51 (00:16:b6:f7:1d:51)  第1跳路由的MAC地址：Destination address: Cisco-Li\_f4:eb:a8 (00:16:b6:f4:eb:a8)  无线主机IP地址：Source Address: 192.168.1.109  目的IP地址：Destination Address: 128.119.245.12  不与任何当前MAC地址对应，因为不在同一“子网”中。      （8）  无线主机MAC地址：Destination address: 91:2a:b0:49:b6:4f (91:2a:b0:49:b6:4f)接入点MAC地址：BSS Id: Cisco-Li\_f7:1d:51 (00:16:b6:f7:1d:51)  第1跳路由的MAC地址：Source address: Cisco-Li\_f4:eb:a8 (00:16:b6:f4:eb:a8)  不对应，不在同一子网中。    （9）发送DHCP Release报文以及802.11 Deauthentication类型报文。    （10）通过过滤器我们发现主机只接受到一次linksys AP的Beason帧，其余报文均是同30 Munroe St. AP来往，可能是由于实验材料的版本问题，这些问题不能得到很好的细究。    （11）观察字段Authentication Algorithm: Open System (0)表示主机希望开放系统的认证算法。    （12）无  （13）由下图可见，于63.168087时刻及之前主机不断发送请求帧，于63.169071时刻AP回复。    （14）使用过滤器wlan.fc.subtype < 2 and wlan.fc.type == 0 and wlan.addr == 00:13:02:d1:b6:4f（要使用MAC地址而不是别名）筛选得    （15）    （16）Request帧中：  Receiver address: Broadcast (ff:ff:ff:ff:ff:ff)  Transmitter address: IntelCor\_1f:57:13 (00:12:f0:1f:57:13)  BSS Id: Broadcast (ff:ff:ff:ff:ff:ff)    Response帧中：  Receiver address: IntelCor\_1f:57:13 (00:12:f0:1f:57:13)  Transmitter address: Cisco-Li\_f7:1d:51 (00:16:b6:f7:1d:51)  BSS Id: Cisco-Li\_f7:1d:51 (00:16:b6:f7:1d:51)    用于主机主动扫描周围的AP信号。 | | | |
| 结论分析与体会：  这次实验学习了802.11协议，与之前的协议不同，这个协议是无线的，因而Wireshark也收集了许多通信时物理数据如信号强度、噪声强度等等。之前做过蓝牙相关的安卓开发，在学习了802.11之后对无线通信的许多概念（例如Beacon帧，最初接触，我以为这是一种虚拟路标呢，不过确实也可以这么干哈哈，可以展示一些信息比如图片，现在才知道它本质是AP的广播帧）有了深入的体会。 | | | |