《计算机网络》作业 3

1900017812 高乐耘*

2023 年 4 月 2 日

I. 实验环境

- 操作系统：Ubuntu 22.04.2 LTS (GNU/Linux 5.19.0-38-generic x86_64)

- 网卡：Intel Wireless-AC 9260

- 网络连接：PKU 5.2 GHz 无线校园网

- 浏览器：Mozilla Firefox 111.0.1

- Wireshark：Wireshark 3.6.2 (Git v3.6.2 packaged as 3.6.2-2)

II. 802.11 WiFi 协议分析

A. 信标帧

附页中给出了 Wireshark_802_11.pcap 记录中的第 13 和 14 帧的部分详细信息，它们对应的 SSID 在整个记录内的所有信标帧中出现频率最高。

1. 它们的 SSID 分别为 30 Munroe St 和 linksys12。

2. 它们的信标帧周期均为 0.1024 s。

3. 30 Munroe St 信标帧的源地址为 00:16:b6:f7:1d:51。

4. 30 Munroe St 信标帧的目的地址为 ff:ff:ff:ff:ff:ff，这是一个广播地址。

5. 30 Munroe St 信标帧的 BSS 地址为 00:16:b6:f7:1d:51，在此处与源地址一致。

6. 30 Munroe St 支持 1，2，5.5，11 Mbps 四种基本速率和 6，9，12，18，24，36，48，54 Mbps 八种扩展速率。

B. 数据传输

附页中给出了 Wireshark_802_11.pcap 记录中的第 474 帧的部分详细信息，它对应 $t = 24.82$ 时用户向服务器 128.119.245.12 发起的下载 alice.txt 的 GET 请求的 TCP 连接建立时的第一次握手（SYN）。

---

*电子邮件地址: seeson@pku.edu.cn　手机号: 13759115414

7. 该 802.11 帧中包含了源 MAC 地址 00:13:02:d1:b6:4f（对应主机地址），目的 MAC 地址 00:16:b6:f4:eb:a8（对应第一跳路由器地址）和 BSS MAC 地址 00:16:b6:f7:1d:51（对应接入点地址）。源 IP 地址为 192.168.1.109，目标 IP 地址为 128.119.245.12。目标 IP 地址对应服务器 gaia.cs.umass.edu，本地主机通过 TCP/IP 协议向其发送包含 TCP 报文的 IP 分组以传输 HTTP GET 请求来获取所需的 alice.txt 的内容，故此处的目的 IP 地址需要填写对方服务器的 IP 地址。

附页中给出了 Wireshark_802_11.pcap 记录中的第 476 帧的部分详细信息，它对应服务器 128.119.245.12 对 $t = 24.82$ 时用户发起的下载 alice.txt 的 GET 请求的 TCP 连接建立时的第二次握手（SYN，ACK）。

8. 该 802.11 帧中包含了源 MAC 地址 00:16:b6:f4:eb:a8（对应第一跳路由器地址），目的 MAC 地址 91:2a:b0:49:b6:4f（对应主机地址，但结合其它捕获的帧来看这一地址并不正确，大量结果表明正确的主机地址应为 00:13:02:d1:b6:4f）和 BSS MAC 地址 00:16:b6:f7:1d:51（对应接入点地址）。该帧发送方 MAC 地址不与最初发送该帧封装的 TCP 报文的服务器的 IP 地址对应，而是与转发该帧的最后一跳路由器（从本机视角看是第一跳路由器）的 IP 地址对应。

C. 关联与解除关联

应用显示过滤器

wlan.fc.type == 0 and (wlan.fc.subtype == 0 or wlan.fc.subtype == 1)

选择所有关联请求和关联响应帧。应用显示过滤器

wlan.fc.type == 0 and (wlan.fc.subtype == 10 or wlan.fc.subtype == 12)

选择所有解除关联和解除身份验证帧。应用显示过滤器

wlan.fc.type == 0 and wlan.fc.subtype == 11

选择所有身份验证帧。

9. 应用上述显示过滤器选择所有解除关联和解除身份验证帧，仅有一个候选项捕获时间接近第 49 秒，为第 1735 帧，这是一个解除身份验证帧，如图 1。清空显示过滤器，从第 1735 帧向前寻找，在不远处（第 1733 帧）找到一 DHCP 释放 IP 地址的报文，如图 2。在列表中未见 $t = 49$ 前后本机发出任何解除关联帧，可能是本机发送的解除身份验证帧（第 1735 帧）已经包含了其语义。

10. 应用上述显示过滤器选择所有身份验证帧，看到 $t \approx 49$ s 起共有 15 个身份验证帧发往 Cisco_Li_f5:ba:bb，如图 3。

11. 本地主机希望对方 AP 提供的 BSS 是开放（即不加密）的，如附页中的第 1740 帧（$t \approx 49$ s 时首个发往 Cisco_Li_f5:ba:bb 的身份验证帧）中显示的详细信息。
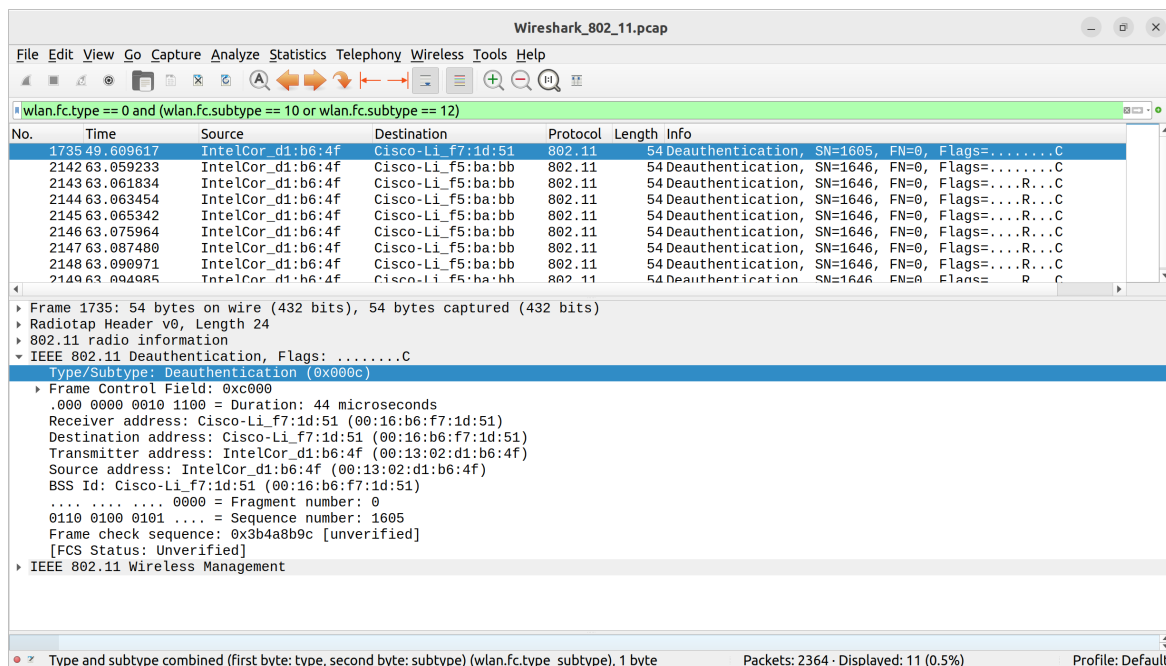
12. 对方 AP 没有回复任何身份验证帧。

图 1: Wireshark 显示的 Wireshark_802_11.pcap 记录中的帧列表，应用了选择所有解除关联和解除身份验证帧的过滤器。选中帧（编号 1735）为唯一可能的与首次断开 WiFi 连接相关的解除关联或解除身份验证帧。
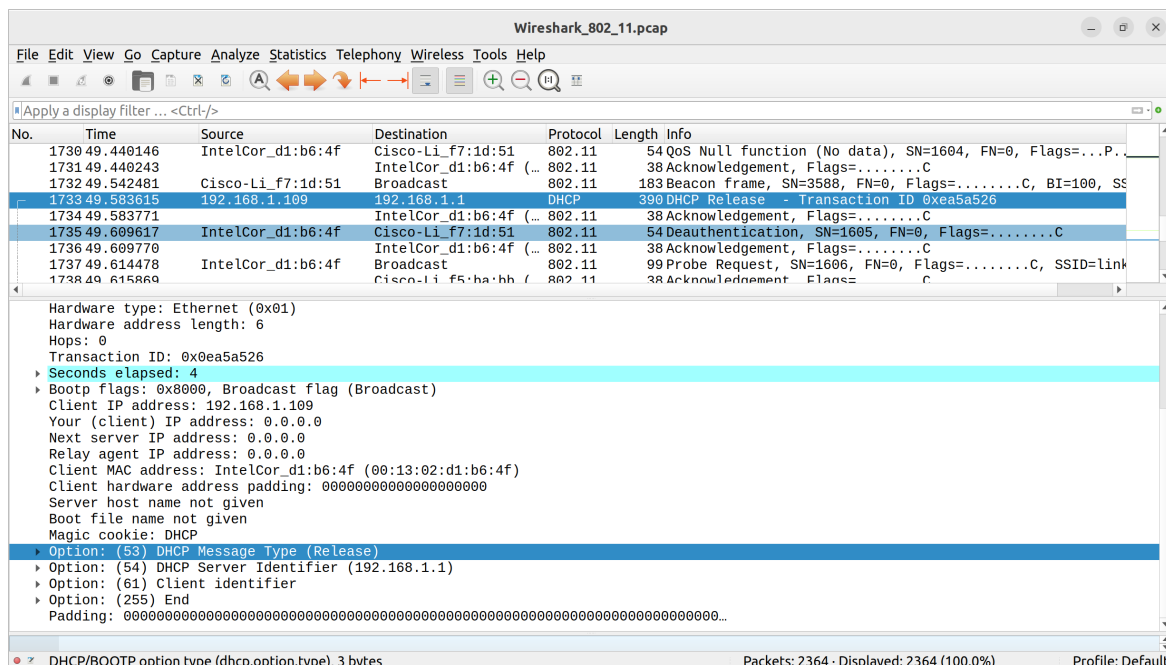

图 2: Wireshark 显示的 Wireshark_802_11.pcap 记录中的帧列表，选中的帧（第 1733 帧）中包含了在第 1735 帧（鼠标悬停处）前的附近找到的本机向 DHCP 服务器发送的释放 IP 地址占用的 UDP 报文。

图 3: Wireshark 显示的 Wireshark_802_11.pcap 记录中的帧列表，应用了选择所有身份验证帧的过滤器。$t \approx 49$ s 起共有 15 个身份验证帧发往 Cisco_Li_f5:ba:bb。

图 4: Wireshark 显示的 Wireshark_802_11.pcap 记录中的帧列表，应用了选择所有关联请求和关联响应帧的过滤器，仅选中的两帧源或目标地址中包括 00:16:b6:f7:1d:51，对应的 SSID 为 30 Munroe St。

图 5: Wireshark 显示的 Wireshark_802_11.pcap 记录中的帧列表，其中鼠标选中的为本机与 30 Munroe St 之间发送的身份认证帧，鼠标悬停处为本机向该 AP 发送的关联请求帧，它们之间呈交错关系。

13. 从图 3 中可见，$t = 63.168087$ 时本机向 30 Munroe St AP 发送身份认证帧，$t = 63.169071$ 时对方回复，$t = 63.169707$ 时本机再次发送，$t = 63.170692$ 时对方再次回复。双方共发送 4 个身份认证帧。

14. 应用上述显示过滤器选择所有关联请求和关联响应帧，与 00:16:b6:f7:1d:51 相关的只有第 2162 和第 2166 帧，如图 4。它们的捕获时间分别为 63.169910 和 63.192101。从图 5 中还看到，关联请求帧与 4 个身份认证帧是交错的，关联请求出现在 3 个身份认证帧之后，其后还跟着 1 个身份认证帧。

15. 附页中给出了第 2162 和第 2166 帧的详细信息，从中看出本地主机支持的速率包括：

pported Rates 1(B)，2(B)，5.5(B)，11(B)，6(B)，9，12(B)，18，[Mbit/sec]
tended Supported Rates 24(B)，36，48，54，[Mbit/sec]

AP 支持的速率包括：

pported Rates 1(B)，2(B)，5.5(B)，11(B)，[Mbit/sec]
tended Supported Rates 6(B)，9，12(B)，18，24(B)，36，48，54，[Mbit/sec]

D. 其它帧类型

应用显示过滤器

wlan.fc.type == 0 and (wlan.fc.subtype == 4 or wlan.fc.subtype == 5)

选择所有关联请求和关联响应帧。
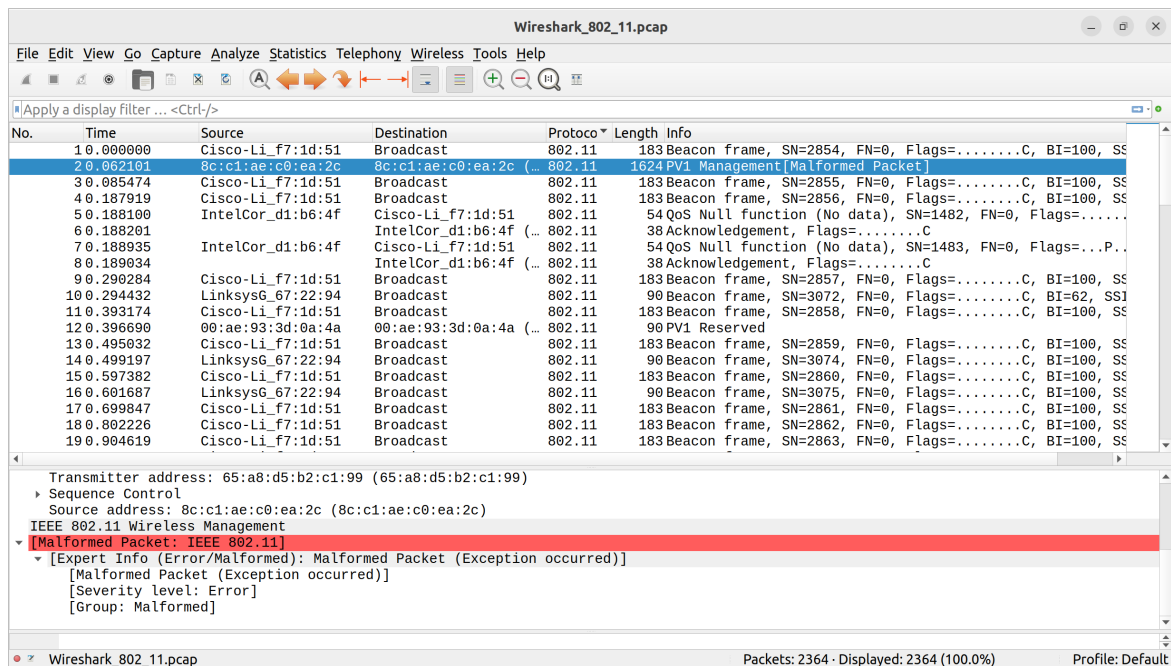
图 6: Wireshark_802_11.pcap 中包含的错帧之一，帧序号为 2，其中红色标识了无法识别的分组内容。

16. 应用上述显示过滤器，查找到众多结果。以第 50 和 51 帧为例（详细信息见附页），第 50 帧为探测请求帧，发送者的 MAC 为 IntelCor_1f:57:13（本机），接收者的 MAC 为 ff:ff:ff:ff:ff:ff（广播地址），BSS ID 的 MAC 为 ff:ff:ff:ff:ff:ff（广播地址）；第 51 帧为探测响应帧，发送者为 Cisco-Li_f7:1d:51（SSID 为 30 Munroe St 的 AP），接收者为 IntelCor_1f:57:13（本机），BSS ID MAC 与发送者相同，为该 AP 地址。探测请求帧用于客户端以主动方式对信道内的 AP 进行扫描，AP 如果回应探测响应帧，则可能被发送探测请求的主机探测到，并可能在将来收到该主机的关联请求。

E. 错帧

Wireshark_802_11.pcap 中存在不少错帧，以图 6 为例。同时，Wireshark 显示并未使用帧头的 FCS 对帧头进行校验，所以实际上很可能包含了更大数量的错帧。之前提到的错误主机地址说明了这一点，它所在的帧并未直接被标记为错帧。

III. 信号强度与数据率之间关系的分析

考虑使用 iwconfig 工具来获得数据率（DR）和接收信号强度（RSS）。使用 Redmi 9 手机发射 WiFi 信号 lyazj，在笔记本电脑上连接该 WiFi 后，执行 iwconfig wlp1s0，输出如下：

```
wlp1s0    IEEE 802.11   ESSID:"lyazj"
          Mode:Managed   Frequency:2.437 GHz   Access Point: 76:14:7E:68:67:1B
          Bit Rate=72.2 Mb/s    Tx-Power=22 dBm
          Retry short limit:7   RTS thr:off   Fragment thr:off
          Power Management:on
          Link Quality=70/70   Signal level=-26 dBm
```

```
          Rx invalid nwid:0  Rx invalid crypt:0  Rx invalid frag:0
          Tx excessive retries:2  Invalid misc:72    Missed beacon:0
```

从中可以读出比特率为 72.2 Mb/s，信号水平为 −26 dBm。下面的 Python 程序实现了在 `scan_period` 秒内，每隔 `scan_interval` 秒采集一次 iwconfig wlp1s0 结果，并输出至文件 `output_npz` 的功能：

```python
#!/usr/bin/env python3

import re
import os
import numpy as np
import time

# Configuration.
iwconfig_command = 'iwconfig wlp1s0'
scan_period = 60
scan_interval = 0.1
output_npz = 'dr-rss.npz'

# String patterns to parse iwconfig output.
re_dr = re.compile(r'Bit Rate=\s*(.*?)\s*b/s', re.M)
re_rss = re.compile(r'Signal level=\s*(.*?)\s*dBm', re.M)

# Execute 'iwconfig_command' and return (DR (b/s), RSS (dBm)).
def run_iwconfig() -> map:
    with os.popen(iwconfig_command, 'r') as p:
        output = p.read()
    return map(lambda e: e.search(output).group(1), (re_dr, re_rss))

# Convert the string encoded DR to float (bps).
def parse_dr(dr: str) -> float:
    dr = dr.split(' ')
    number = float(dr[0])
    unit = 1.0 if len(dr) == 1 else {
        'K': 1e3,
        'M': 1e6,
        'G': 1e9,
        'T': 1e12,
    }[dr[1]]
    return number * unit

# Convert the string encoded RSS to float (dBm).
def parse_rss(rss: str) -> float:
    return float(rss)

# Invoke run_iwconfig() and parse_*() to get current DR and RSS.
def get_dr_rss() -> (float, float):
    dr, rss = run_iwconfig()
    dr = parse_dr(dr)
```
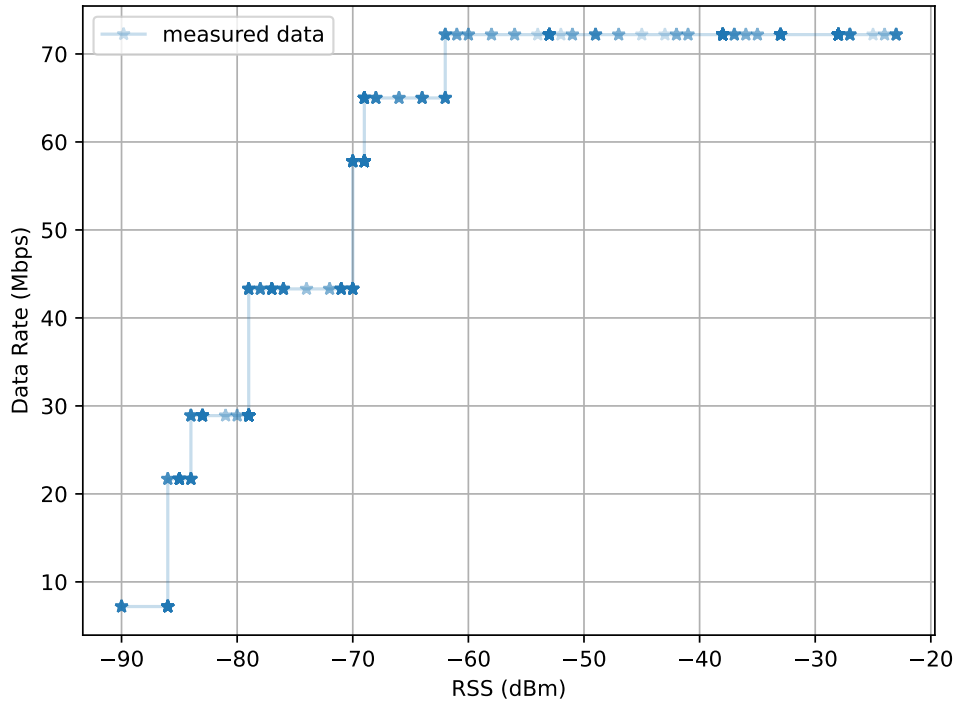
图 7：改变手机与电脑之间的距离采集到的接收信号强度（RSS）和数据率（DR）的多组数据（五角星）及其排序之后的连线（直线）。共有 $(60 // 0.1) + 1 = 600$（Python 给出的计算结果，由于浮点误差并非 601）个数据点，均以五角星表示，由于大量数据点重合，图层叠加后看到的五角星数量远不足 600，但在 75% 的透明度下重叠数目的相对多少清晰可见。

```
    rss = parse_rss(rss)
    return dr, rss


# Scan DR and RSS for 'period' secs, with an interval of 'interval' secs.
# Return an np.array of shape (int(period // interval) + 1, 2).
def scan_dr_rss(period: float, interval: float) -> np.array:
    n = int(period // interval)
    data = np.empty(shape=(n + 1, 2))
    data[0] = get_dr_rss()
    print(0, '/', n, '  ', data[0][0], 'bps', '  ', data[0][1], 'dBm')
    for i in range(1, n + 1):
        time.sleep(interval)
        data[i] = get_dr_rss()
        print(i, '/', n, '  ', data[i][0], 'bps', '  ', data[i][1], 'dBm')
    return data


if __name__ == '__main__':
    # Do the scanning and save the data to 'output_npz'.
    np.savez(output_npz, data=scan_dr_rss(scan_period, scan_interval))
```

保持电脑和手机之间的 WiFi 信号连接，设置扫描时长 60 秒，扫描间隔 0.1 秒，手持手机由近即远，又由远即近地改变与笔记本电脑之间的距离，获得不同信号强度下的数据率。其结果绘制于图 7 中。分析这一结果，可以得到以下几点结论：

8

- 数据率随接收信号强度的增大而阶梯式递增，保持单调，在本次实验中没有显示出明显的后效性

- 本实验测得的最小数据率为 7.2 Mbps（对应的 RSS 为 −90 dBm 附近），最大数据率为 72.2 Mbps（对应的 RSS 为 −23 dBm 附近）

- 实验观测到的数据率阶梯包括 7.2, 21.7, 28.9, 43.3, 57.8, 65.0, 72.2 (Mbps)，但由于各种变化因素，这一结果并不保证是完备的

- 从每一阶梯占有的信号强度区间宽度上看，数据率阶梯是不等宽的，且其宽度分布未见明显规律

- 在控制误码率的意义下，高信号强度是高数据率的前提，实际部署无线网络时应妥善考虑并实际测试各接入设备位置处的信号强度，避免在无线数据链路上引入带宽瓶颈

参考文献

[1] Kurose, J. F., Ross, K. W. (2021). Computer Networking: A Top-Down Approach. Boston, MA: Pearson. ISBN: 978-0-13-592861-5.

```
No.     Time              Source                Destination            Protocol Length Info
      13 0.495032         Cisco-Li_f7:1d:51     Broadcast              802.11   183    Beacon frame, SN=2859, FN=0,
Flags=........C, BI=100, SSID=30 Munroe St
Frame 13: 183 bytes on wire (1464 bits), 183 bytes captured (1464 bits)
Radiotap Header v0, Length 24
802.11 radio information
IEEE 802.11 Beacon frame, Flags: ........C
     Type/Subtype: Beacon frame (0x0008)
     Frame Control Field: 0x8000
     .000 0000 0000 0000 = Duration: 0 microseconds
     Receiver address: Broadcast (ff:ff:ff:ff:ff:ff)
     Destination address: Broadcast (ff:ff:ff:ff:ff:ff)
     Transmitter address: Cisco-Li_f7:1d:51 (00:16:b6:f7:1d:51)
     Source 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)
     .... .... .... 0000 = Fragment number: 0
     1011 0010 1011 .... = Sequence number: 2859
     Frame check sequence: 0xbc03354d [unverified]
     [FCS Status: Unverified]
IEEE 802.11 Wireless Management
     Fixed parameters (12 bytes)
         Timestamp: 174319513986
         Beacon Interval: 0.102400 [Seconds]
         Capabilities Information: 0x0601
     Tagged parameters (119 bytes)
         Tag: SSID parameter set: 30 Munroe St
         Tag: Supported Rates 1(B), 2(B), 5.5(B), 11(B), [Mbit/sec]
         Tag: DS Parameter set: Current Channel: 6
         Tag: Traffic Indication Map (TIM): DTIM 0 of 1 bitmap
         Tag: Country Information: Country Code US, Environment Indoor
         Tag: EDCA Parameter Set
         Tag: ERP Information
         Tag: Extended Supported Rates 6(B), 9, 12(B), 18, 24(B), 36, 48, 54, [Mbit/sec]
         Tag: Vendor Specific: Airgo Networks, Inc.
         Tag: Vendor Specific: Microsoft Corp.: WMM/WME: Parameter Element
```

```
No.      Time              Source                Destination           Protocol  Length  Info
     14 0.499197          LinksysG_67:22:94      Broadcast             802.11    90      Beacon frame, SN=3074, FN=0,
Flags=........C, BI=100, SSID=linksys12
Frame 14: 90 bytes on wire (720 bits), 90 bytes captured (720 bits)
Radiotap Header v0, Length 24
802.11 radio information
IEEE 802.11 Beacon frame, Flags: ........C
    Type/Subtype: Beacon frame (0x0008)
    Frame Control Field: 0x8000
    .000 0000 0000 0000 = Duration: 0 microseconds
    Receiver address: Broadcast (ff:ff:ff:ff:ff:ff)
    Destination address: Broadcast (ff:ff:ff:ff:ff:ff)
    Transmitter address: LinksysG_67:22:94 (00:06:25:67:22:94)
    Source address: LinksysG_67:22:94 (00:06:25:67:22:94)
    BSS Id: 50:2b:25:67:22:94 (50:2b:25:67:22:94)
    .... .... .... 0000 = Fragment number: 0
    1100 0000 0010 .... = Sequence number: 3074
    Frame check sequence: 0x5d5654a6 [unverified]
    [FCS Status: Unverified]
IEEE 802.11 Wireless Management
    Fixed parameters (12 bytes)
        Timestamp: 9534921933578
        Beacon Interval: 0.102400 [Seconds]
        Capabilities Information: 0x0011
    Tagged parameters (26 bytes)
        Tag: SSID parameter set: linksys12
        Tag: Supported Rates 1(B), 2(B), 5.5, 11, [Mbit/sec]
        Tag: DS Parameter set: Current Channel: 6
        Tag: Traffic Indication Map (TIM): DTIM 2 of 3 bitmap
```

```
No.      Time          Source                Destination           Protocol Length Info
     474 24.811093     192.168.1.109         128.119.245.12        TCP      110    2538 → 80 [SYN] Seq=0
Win=16384 Len=0 MSS=1460 SACK_PERM=1
Frame 474: 110 bytes on wire (880 bits), 110 bytes captured (880 bits)
Radiotap Header v0, Length 24
802.11 radio information
IEEE 802.11 QoS Data, Flags: .......TC
    Type/Subtype: QoS Data (0x0028)
    Frame Control Field: 0x8801
    .000 0000 0010 1100 = Duration: 44 microseconds
    Receiver address: Cisco-Li_f7:1d:51 (00:16:b6:f7:1d:51)
    Transmitter address: IntelCor_d1:b6:4f (00:13:02:d1:b6:4f)
    Destination address: Cisco-Li_f4:eb:a8 (00:16:b6:f4:eb:a8)
    Source address: IntelCor_d1:b6:4f (00:13:02:d1:b6:4f)
    BSS Id: Cisco-Li_f7:1d:51 (00:16:b6:f7:1d:51)
    STA address: IntelCor_d1:b6:4f (00:13:02:d1:b6:4f)
    .... .... .... 0000 = Fragment number: 0
    0000 0011 0001 .... = Sequence number: 49
    Frame check sequence: 0xad57fce0 [unverified]
    [FCS Status: Unverified]
    Qos Control: 0x0000
Logical-Link Control
Internet Protocol Version 4, Src: 192.168.1.109, Dst: 128.119.245.12
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
    Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 48
    Identification: 0x1324 (4900)
    Flags: 0x40, Don't fragment
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 128
    Protocol: TCP (6)
    Header Checksum: 0xb00a [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.168.1.109
    Destination Address: 128.119.245.12
Transmission Control Protocol, Src Port: 2538, Dst Port: 80, Seq: 0, Len: 0
    Source Port: 2538
    Destination Port: 80
    [Stream index: 0]
    [Conversation completeness: Complete, WITH_DATA (31)]
    [TCP Segment Len: 0]
    Sequence Number: 0    (relative sequence number)
    Sequence Number (raw): 1907346758
    [Next Sequence Number: 1    (relative sequence number)]
    Acknowledgment Number: 0
    Acknowledgment number (raw): 0
    0111 .... = Header Length: 28 bytes (7)
    Flags: 0x002 (SYN)
    Window: 16384
    [Calculated window size: 16384]
    Checksum: 0xc255 [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
    Options: (8 bytes), Maximum segment size, No-Operation (NOP), No-Operation (NOP), SACK permitted
    [Timestamps]
```

```
No.     Time            Source              Destination         Protocol Length Info
    476 24.827751       128.119.245.12      192.168.1.109       TCP      110     80 → 2538 [SYN, ACK] Seq=0
Ack=1 Win=5840 Len=0 SACK_PERM=1
Frame 476: 110 bytes on wire (880 bits), 110 bytes captured (880 bits)
Radiotap Header v0, Length 24
802.11 radio information
IEEE 802.11 QoS Data, Flags: ..mP..F.C
    Type/Subtype: QoS Data (0x0028)
    Frame Control Field: 0x8832
    Duration/ID: 11560 (reserved)
    Receiver address: 91:2a:b0:49:b6:4f (91:2a:b0:49:b6:4f)
    Transmitter address: Cisco-Li_f7:1d:51 (00:16:b6:f7:1d:51)
    Destination address: 91:2a:b0:49:b6:4f (91:2a:b0:49:b6:4f)
    Source address: Cisco-Li_f4:eb:a8 (00:16:b6:f4:eb:a8)
    BSS Id: Cisco-Li_f7:1d:51 (00:16:b6:f7:1d:51)
    STA address: 91:2a:b0:49:b6:4f (91:2a:b0:49:b6:4f)
    .... .... .... 0000 = Fragment number: 0
    1100 0011 0100 .... = Sequence number: 3124
    Frame check sequence: 0xecdc407d [unverified]
    [FCS Status: Unverified]
    Qos Control: 0x0100
Logical-Link Control
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.109
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
    Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 48
    Identification: 0x0000 (0)
    Flags: 0x40, Don't fragment
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 49
    Protocol: TCP (6)
    Header Checksum: 0x122f [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 128.119.245.12
    Destination Address: 192.168.1.109
Transmission Control Protocol, Src Port: 80, Dst Port: 2538, Seq: 0, Ack: 1, Len: 0
    Source Port: 80
    Destination Port: 2538
    [Stream index: 0]
    [Conversation completeness: Complete, WITH_DATA (31)]
    [TCP Segment Len: 0]
    Sequence Number: 0     (relative sequence number)
    Sequence Number (raw): 2928664127
    [Next Sequence Number: 1     (relative sequence number)]
    Acknowledgment Number: 1     (relative ack number)
    Acknowledgment number (raw): 1907346759
    0111 .... = Header Length: 28 bytes (7)
    Flags: 0x012 (SYN, ACK)
    Window: 5840
    [Calculated window size: 5840]
    Checksum: 0x5ea5 [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 208
    Options: (8 bytes), CC.ECHO, No-Operation (NOP), No-Operation (NOP), SACK permitted
    [Timestamps]
    [SEQ/ACK analysis]
```

```
No.      Time              Source             Destination           Protocol Length Info
   1740 49.638857         IntelCor_d1:b6:4f   Cisco-Li_f5:ba:bb     802.11   58     Authentication, SN=1606,
FN=0, Flags=........C
Frame 1740: 58 bytes on wire (464 bits), 58 bytes captured (464 bits)
Radiotap Header v0, Length 24
802.11 radio information
IEEE 802.11 Authentication, Flags: ........C
IEEE 802.11 Wireless Management
    Fixed parameters (6 bytes)
        Authentication Algorithm: Open System (0)
        Authentication SEQ: 0x0001
        Status code: Successful (0x0000)
```

```
No.      Time            Source              Destination           Protocol Length Info
   2162 63.169910       IntelCor_d1:b6:4f    Cisco-Li_f7:1d:51     802.11   89     Association Request,
SN=1648, FN=0, Flags=........C, SSID=30 Munroe St
Frame 2162: 89 bytes on wire (712 bits), 89 bytes captured (712 bits)
Radiotap Header v0, Length 24
802.11 radio information
IEEE 802.11 Association Request, Flags: ........C
IEEE 802.11 Wireless Management
    Fixed parameters (4 bytes)
    Tagged parameters (33 bytes)
        Tag: SSID parameter set: 30 Munroe St
        Tag: Supported Rates 1(B), 2(B), 5.5(B), 11(B), 6(B), 9, 12(B), 18, [Mbit/sec]
        Tag: QoS Capability
        Tag: Extended Supported Rates 24(B), 36, 48, 54, [Mbit/sec]
```

```
No.      Time            Source                Destination          Protocol Length Info
 2166 63.192101        Cisco-Li_f7:1d:51     IntelCor_d1:b6:4f      802.11   94     Association Response,
SN=3728, FN=0, Flags=........C
Frame 2166: 94 bytes on wire (752 bits), 94 bytes captured (752 bits)
Radiotap Header v0, Length 24
802.11 radio information
IEEE 802.11 Association Response, Flags: ........C
IEEE 802.11 Wireless Management
    Fixed parameters (6 bytes)
    Tagged parameters (36 bytes)
        Tag: Supported Rates 1(B), 2(B), 5.5(B), 11(B), [Mbit/sec]
        Tag: Extended Supported Rates 6(B), 9, 12(B), 18, 24(B), 36, 48, 54, [Mbit/sec]
        Tag: EDCA Parameter Set
```

```
No.      Time            Source                  Destination             Protocol Length Info
     50 2.297613         IntelCor_1f:57:13       Broadcast               802.11   79      Probe Request, SN=576, FN=0,
Flags=........C, SSID=Home WIFI
Frame 50: 79 bytes on wire (632 bits), 79 bytes captured (632 bits)
Radiotap Header v0, Length 24
802.11 radio information
IEEE 802.11 Probe Request, Flags: ........C
    Type/Subtype: Probe Request (0x0004)
    Frame Control Field: 0x4000
    .000 0000 0000 0000 = Duration: 0 microseconds
    Receiver address: Broadcast (ff:ff:ff:ff:ff:ff)
    Destination address: Broadcast (ff:ff:ff:ff:ff:ff)
    Transmitter address: IntelCor_1f:57:13 (00:12:f0:1f:57:13)
    Source address: IntelCor_1f:57:13 (00:12:f0:1f:57:13)
    BSS Id: Broadcast (ff:ff:ff:ff:ff:ff)
    .... .... .... 0000 = Fragment number: 0
    0010 0100 0000 .... = Sequence number: 576
    Frame check sequence: 0xa373c5ff [unverified]
    [FCS Status: Unverified]
IEEE 802.11 Wireless Management
```

```
No.      Time            Source              Destination         Protocol Length Info
      51 2.300697        Cisco-Li_f7:1d:51   IntelCor_1f:57:13   802.11   177    Probe Response, SN=2878,
FN=0, Flags=........C, BI=100, SSID=30 Munroe St
Frame 51: 177 bytes on wire (1416 bits), 177 bytes captured (1416 bits)
Radiotap Header v0, Length 24
802.11 radio information
IEEE 802.11 Probe Response, Flags: ........C
    Type/Subtype: Probe Response (0x0005)
    Frame Control Field: 0x5000
    .000 0001 0011 1010 = Duration: 314 microseconds
    Receiver address: IntelCor_1f:57:13 (00:12:f0:1f:57:13)
    Destination address: IntelCor_1f:57:13 (00:12:f0:1f:57:13)
    Transmitter address: Cisco-Li_f7:1d:51 (00:16:b6:f7:1d:51)
    Source 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)
    .... .... .... 0000 = Fragment number: 0
    1011 0011 1110 .... = Sequence number: 2878
    Frame check sequence: 0x6ed851bb [unverified]
    [FCS Status: Unverified]
IEEE 802.11 Wireless Management
```