

**ĐẠI HỌC QUỐC GIA THÀNH PHỐ HỒ CHÍ MINH**  
**TRƯỜNG ĐẠI HỌC BÁCH KHOA**  
**KHOA KHOA HỌC VÀ KỸ THUẬT MÁY TÍNH**



**MẠNG MÁY TÍNH TN (CO3094)**

**LAB 7**

**Wireshark Lab: 802.11 WiFi v8.0**

**HK: 241 - LỚP: L09**

**GVHD: Bùi Xuân Giang**

**Sinh viên thực hiện**

**Nguyễn Tấn Tài : 2212990**

Thành phố Hồ Chí Minh, tháng 11 năm 2024

## Wireshark Lab: 802.11 WiFi v8.0

Trong bài thực hành này, chúng ta sẽ tìm hiểu về giao thức mạng không dây 802.11. Trước khi bắt đầu bài thực hành này, bạn có thể muốn đọc lại Phần 7.3 trong sách giáo khoa. Vì chúng ta sẽ đi sâu vào chi tiết của 802.11 hơn so với phần trình bày trong sách, bạn có thể muốn tham khảo “A Technical Tutorial on the 802.11 Protocol” của Pablo Brenner (Breezecom Communications), [http://www.sss-mag.com/pdf/802\\_11tut.pdf](http://www.sss-mag.com/pdf/802_11tut.pdf), và “Understanding 802.11 Frame Types” của Jim Geier, <http://www.wi-fiplanet.com/tutorials/article.php/1447501>. Và, tất nhiên, còn có “kinh thánh” về 802.11 - tiêu chuẩn chính nó, “ANSI/IEEE Std 802.11, 1999 Edition (R2003),” <http://gaia.cs.umass.edu/wireshark-labs/802.11-1999.pdf>. Trong tài liệu này, bạn có thể tìm thấy Bảng 1 trên trang 36 của tiêu chuẩn đặc biệt hữu ích khi xem qua các gói tin không dây.

Trong tất cả các bài thực hành Wireshark trước đây, chúng ta đã thu thập các khung trên kết nối Ethernet có dây. Tuy nhiên, vì 802.11 là một giao thức liên kết không dây, chúng ta sẽ thu thập các khung “trong không khí.” Không may thay, một số trình điều khiển thiết bị cho giao diện không dây 802.11 NICs vẫn không cung cấp các móc nối để thu thập/sao chép các khung 802.11 nhận được cho sử dụng trong Wireshark (xem Hình 1 trong Bài 1 để có tổng quan về việc thu thập gói tin). Vì vậy, trong bài thực hành này, chúng tôi sẽ cung cấp một tập hợp các gói tin 802.11 đã thu thập để bạn phân tích và giả định trong các câu hỏi dưới đây rằng bạn đang sử dụng tập gói tin này. Nếu bạn có thể thu thập các khung 802.11 bằng phiên bản Wireshark của mình, bạn được hoan nghênh làm điều đó.

### 1. Getting Started

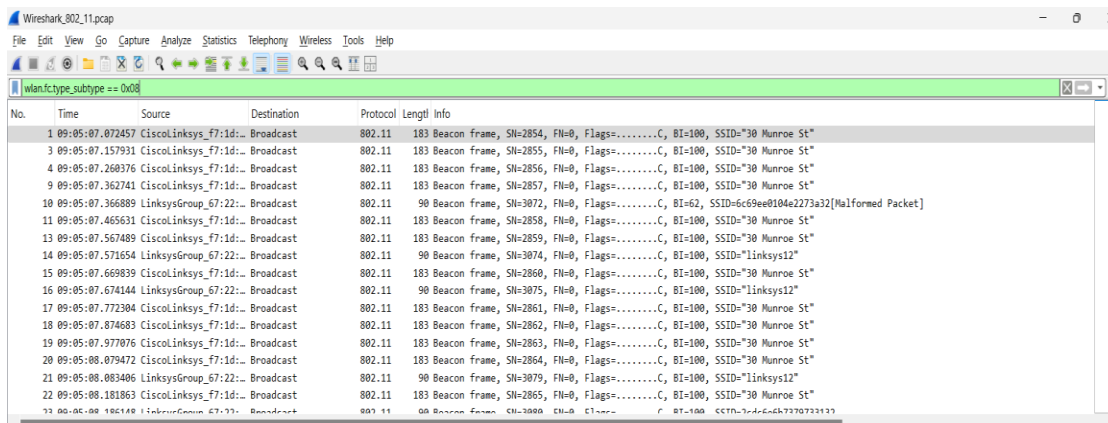
Tải xuống file zip từ <http://gaia.cs.umass.edu/wireshark-labs/wireshark-traces.zip> và giải nén file *Wireshark\_802\_11.pcap*. Tập gói tin này được thu thập bằng AirPcap và Wireshark chạy trên một máy tính tại mạng gia đình của một trong những tác giả, bao gồm bộ định tuyến (router) kết hợp điểm truy cập (access point) không dây Linksys 802.11g, với hai máy tính có dây và một máy chủ không dây PC gắn với bộ định tuyến. Tác giả may mắn có các điểm truy cập trong các ngôi nhà lân cận có thể truy cập được. Trong tập vết

gói tin này, chúng ta sẽ thấy các khung được thu thập trên kênh 6. Vì điểm truy cập và thiết bị của chúng ta không phải là những thiết bị duy nhất sử dụng kênh 6, chúng ta sẽ thấy nhiều khung không liên quan cho bài thực hành này, như các khung beacon được phát ra bởi một điểm truy cập của hàng xóm cũng sử dụng kênh 6.

Các hoạt động của thiết bị không dây được ghi nhận trong tập tin vết này bao gồm:

- Tại  $t = 24.82$  giây, thiết bị thực hiện một yêu cầu HTTP tới <http://gaia.cs.umass.edu/wireshark-labs/alice.txt>. Địa chỉ IP của [gaia.cs.umass.edu](http://gaia.cs.umass.edu) là 128.119.245.12.
- Tại  $t = 32.82$  giây, thiết bị thực hiện một yêu cầu HTTP tới <http://www.cs.umass.edu>, có địa chỉ IP là 128.119.240.19.
- Tại  $t = 49.58$  giây, thiết bị ngắt kết nối khỏi 30 Munroe St và cố gắng kết nối tới linksys\_ses\_24086. Đây không phải là một điểm truy cập mở, vì vậy thiết bị cuối cùng không thể kết nối với điểm truy cập này.
- Tại  $t = 63.0$  giây, thiết bị từ bỏ nỗ lực kết nối với linksys\_ses\_24086 và kết nối lại với điểm truy cập 30 Munroe St.

Khi bạn đã tải xuống tập vết này, bạn có thể tải nó vào Wireshark và xem tập vết bằng cách chọn mục *File* trong thanh menu, chọn *Open*, sau đó chọn tập vết *Wireshark\_802\_11.pcap*. Màn hình hiển thị kết quả sẽ trông giống như Hình 1.

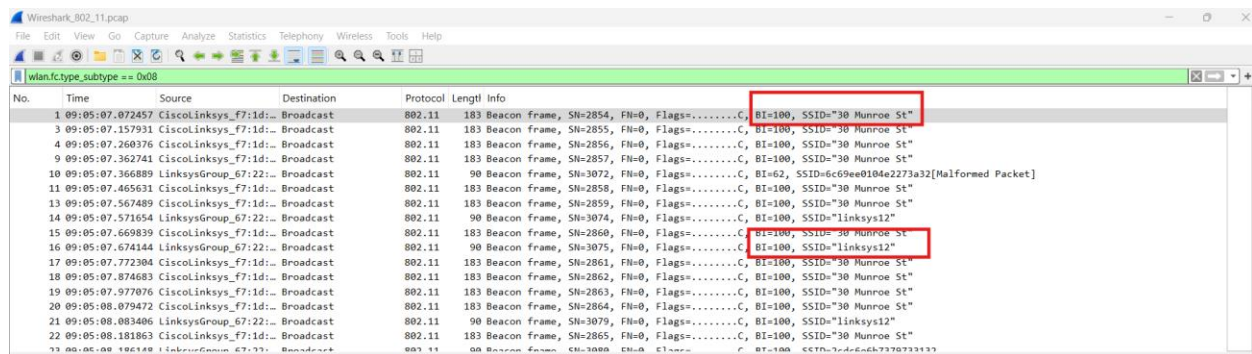


Hình 1 Wireshark window, after opening the Wireshark\_802\_11.pcap file.

## 2. Khung Beacon

Nhớ lại rằng các khung beacon được sử dụng bởi một điểm truy cập (AP) 802.11 để quảng bá sự tồn tại của nó. Để trả lời một số câu hỏi dưới đây, bạn sẽ muốn xem chi tiết của khung “IEEE 802.11” và các trường phụ trong cửa sổ giữa của Wireshark. Khi có thể, khi trả lời một câu hỏi bên dưới, bạn nên in ra một bản của các gói tin mà bạn sử dụng để trả lời câu hỏi. Ghi chú trên bản in này để giải thích câu trả lời của bạn. Để in một gói tin, chọn File->Print, sau đó chọn Selected packet only, chọn Packet summary line, và chọn lượng chi tiết tối thiểu của gói tin mà bạn cần để trả lời câu hỏi.

**Câu 1:** SSID của hai điểm truy cập phát hầu hết các khung beacon trong vết này là gì?



No.	Time	Source	Destination	Protocol	Length	Info
1	09:05:07.072457	CiscoLinksys_f7:1d:...	Broadcast	802.11	183	Beacon frame, Sn=2854, Fn=0, Flags=.....C, BI=100, SSID="30 Munroe St"
3	09:05:07.157931	CiscoLinksys_f7:1d:...	Broadcast	802.11	183	Beacon frame, Sn=2855, Fn=0, Flags=.....C, BI=100, SSID="30 Munroe St"
4	09:05:07.260376	CiscoLinksys_f7:1d:...	Broadcast	802.11	183	Beacon frame, Sn=2856, Fn=0, Flags=.....C, BI=100, SSID="30 Munroe St"
9	09:05:07.362741	CiscoLinksys_f7:1d:...	Broadcast	802.11	183	Beacon frame, Sn=2857, Fn=0, Flags=.....C, BI=100, SSID="30 Munroe St"
10	09:05:07.366889	LinksysGroup_67:22:...	Broadcast	802.11	90	Beacon frame, Sn=3072, Fn=0, Flags=.....C, BI=62, SSID=6c09ee0104e2273a32[Malformed Packet]
11	09:05:07.465631	CiscoLinksys_f7:1d:...	Broadcast	802.11	183	Beacon frame, Sn=2858, Fn=0, Flags=.....C, BI=100, SSID="30 Munroe St"
13	09:05:07.567489	CiscoLinksys_f7:1d:...	Broadcast	802.11	183	Beacon frame, Sn=2859, Fn=0, Flags=.....C, BI=100, SSID="30 Munroe St"
14	09:05:07.571654	LinksysGroup_67:22:...	Broadcast	802.11	90	Beacon frame, Sn=3074, Fn=0, Flags=.....C, BI=100, SSID="linksys12"
15	09:05:07.669839	CiscoLinksys_f7:1d:...	Broadcast	802.11	183	Beacon frame, Sn=2860, Fn=0, Flags=.....C, BI=100, SSID="30 Munroe St"
16	09:05:07.674144	LinksysGroup_67:22:...	Broadcast	802.11	90	Beacon frame, Sn=3075, Fn=0, Flags=.....C, BI=100, SSID="linksys12"
17	09:05:07.772304	CiscoLinksys_f7:1d:...	Broadcast	802.11	183	Beacon frame, Sn=2861, Fn=0, Flags=.....C, BI=100, SSID="30 Munroe St"
18	09:05:07.874683	CiscoLinksys_f7:1d:...	Broadcast	802.11	183	Beacon frame, Sn=2862, Fn=0, Flags=.....C, BI=100, SSID="30 Munroe St"
19	09:05:07.977076	CiscoLinksys_f7:1d:...	Broadcast	802.11	183	Beacon frame, Sn=2863, Fn=0, Flags=.....C, BI=100, SSID="30 Munroe St"
20	09:05:08.079472	CiscoLinksys_f7:1d:...	Broadcast	802.11	183	Beacon frame, Sn=2864, Fn=0, Flags=.....C, BI=100, SSID="30 Munroe St"
21	09:05:08.083406	LinksysGroup_67:22:...	Broadcast	802.11	90	Beacon frame, Sn=3079, Fn=0, Flags=.....C, BI=100, SSID="linksys12"
22	09:05:08.181863	CiscoLinksys_f7:1d:...	Broadcast	802.11	183	Beacon frame, Sn=2865, Fn=0, Flags=.....C, BI=100, SSID="30 Munroe St"
73	00:00:00.186148	LinksysGroup_67:22:...	Broadcast	802.11	90	Beacon frame, Sn=3080, Fn=0, Flags=.....C, BI=100, SSID="30 Munroe St"

Kiểm tra cột "SSID" trong các khung beacon. Từ hình ảnh, có hai SSID xuất hiện nhiều lần là:

- "30 Munroe St"
- "linksys12"

**Câu 2:** Khoảng thời gian giữa các lần phát khung beacon của điểm truy cập linksys\_ses\_24086 là bao nhiêu? Của điểm truy cập 30 Munroe St là bao nhiêu? (Gợi ý: Khoảng thời gian này có trong chính khung beacon).

```
[WLAN Flags: .....C]
IEEE 802.11 Wireless Management
Fixed parameters (12 bytes)
  Timestamp: 174319001986
  Beacon Interval: 0.102400 [Seconds]
  Capabilities Information: 0x0601
    ....1 = ESS capabilities: Transmitter is an AP
    ....0.. = IBSS status: Transmitter belongs to a BSS
    ....0.. = Reserved: 0
    ....0.. = Reserved: 0
    ....0... = Privacy: Data confidentiality not required
    ....0.. = Short Preamble: Not Allowed
    ....0... = Critical Update Flag: False
    ....0... = Nontransmitted BSSIDs Critical Update Flag: False
    ....0... = Spectrum Management: Not Implemented
    ....1... = QoS: Implemented
    ....1.. = Short Slot Time: In use
    ....0... = Automatic Power Save Delivery: Not Implemented
    ....0... = Radio Measurement: Not Implemented
    ....0... = EPD: Not Implemented
    ....0... = Reserved: 0
    ....0... = Reserved: 0
Tagged parameters (119 bytes)
  Tag: SSID parameter set: "30 Munroe St"
  Tag Number: SSID parameter set (0)
  Tag length: 12
  SSID: "30 Munroe St"
```

Khoảng 102.4 ms.

**Câu 3:** (Dưới dạng ký hiệu thập lục phân) Địa chỉ MAC nguồn trên khung beacon từ 30 Munroe St là gì? Nhớ lại từ Hình 7.13 trong sách rằng địa chỉ nguồn, đích và BSS là ba địa chỉ được sử dụng trong một khung 802.11. Để có phần mô tả chi tiết về cấu trúc khung 802.11, hãy xem phần 7 trong tài liệu tiêu chuẩn IEEE 802.11 được đề cập bên trên.

```
[Preamble: 192µs]
IEEE 802.11 Beacon frame, Flags: .....C
Type/Subtype: Beacon frame (0x0008)
Frame Control Field: 0x8000
  ....00 = Version: 0
  ....00.. = Type: Management frame (0)
  1000 .... = Subtype: 8
Flags: 0x00
  ....00 = DS status: Not leaving DS or network is operating in AD-HOC mode (To DS: 0 From DS: 0)
  ....0.. = More Fragments: This is the last fragment
  ....0... = Retry: Frame is not being retransmitted
  ...0 .... = PWR MGT: STA will stay up
  ..0. .... = More Data: No data buffered
  .0.. .... = Protected flag: Data is not protected
  0... .... = +HTC/Order flag: Not strictly ordered
.000 0000 0000 0000 = Duration: 0 microseconds
Receiver address: Broadcast (ff:ff:ff:ff:ff:ff)
  ....1. .... = LG bit: Locally administered address (this is NOT the factory default)
  ....1. .... = IG bit: Group address (multicast/broadcast)
Destination address: Broadcast (ff:ff:ff:ff:ff:ff)
  ....1. .... = LG bit: Locally administered address (this is NOT the factory default)
  ....1. .... = IG bit: Group address (multicast/broadcast)
Transmitter address: Ciscollinksys_f7:1d:51 (00:16:b6:f7:1d:51)
  ....0. .... = LG bit: Globally unique address (factory default)
  ....0. .... = IG bit: Individual address (unicast)
Source address: Ciscollinksys_f7:1d:51 (00:16:b6:f7:1d:51)
  ....0. .... = LG bit: Globally unique address (factory default)
  ....0. .... = IG bit: Individual address (unicast)
BSS Id: Ciscollinksys_f7:1d:51 (00:16:b6:f7:1d:51)
  ....0. .... = LG bit: Globally unique address (factory default)
  ....0. .... = IG bit: Individual address (unicast)
....0000 = Fragment number: 0
1011 0010 0110 .... = Sequence number: 2854
Frame check sequence: 0x057e2608 [unverified]
[FCFS Status: Unverified]
[WLAN Flags: .....C]
```

Từ hình ảnh, địa chỉ MAC của "30 Munroe St" là **ciscoLinksys\_f7:1d:51**.

**Câu 4:** (Dưới dạng ký hiệu thập lục phân) Địa chỉ MAC đích trên khung beacon từ 30 Munroe St là gì?

```
[Preamble: 192µs]
IEEE 802.11 Beacon frame, Flags: .....C
Type/Subtype: Beacon frame (0x0008)
Frame Control Field: 0x0000
.....00 = Version: 0
.....00.. = Type: Management frame (0)
1000..... = Subtype: 8
Flags: 0x00
.....00 = DS status: Not leaving DS or network is operating in AD-HOC mode (To DS: 0 From DS: 0)
.....0... = More Fragments: This is the last fragment
.....0... = Retry: Frame is not being retransmitted
.....0... = PWR MGT: STA will stay up
.....0... = More Data: No data buffered
.....0... = Protected flag: Data is not protected
.....0... = +HTC/Order flag: Not strictly ordered
.....0000 0000 0000 = Duration: 0 microseconds
Receiver address: Broadcast (ff:ff:ff:ff:ff:ff)
.....1..... = LG bit: Locally administered address (this is NOT the factory default)
.....1..... = IG bit: Group address (multicast/broadcast)
Destination address: Broadcast (ff:ff:ff:ff:ff:ff)
.....1..... = LG bit: Locally administered address (this is NOT the factory default)
.....1..... = IG bit: Group address (multicast/broadcast)
Transmitter address: CiscoLinksys_f7:1d:51 (00:16:b6:f7:1d:51)
.....0..... = LG bit: Globally unique address (factory default)
.....0..... = IG bit: Individual address (unicast)
Source address: CiscoLinksys_f7:1d:51 (00:16:b6:f7:1d:51)
.....0..... = LG bit: Globally unique address (factory default)
.....0..... = IG bit: Individual address (unicast)
BSS Id: CiscoLinksys_f7:1d:51 (00:16:b6:f7:1d:51)
.....0..... = LG bit: Globally unique address (factory default)
.....0..... = IG bit: Individual address (unicast)
.....0000 = Fragment number: 0
1011 0010 0110..... = Sequence number: 2854
Frame check sequence: 0x057e2608 [unverified]
[FCS Status: Unverified]
[MLAN Flags: .....C]
```

Trong khung beacon, kiểm tra trường "Destination Address". Địa chỉ này là địa chỉ broadcast ff:ff:ff:ff:ff:ff

**Câu 5:** (Dưới dạng ký hiệu thập lục phân) Địa chỉ MAC BSS ID trên khung beacon từ 30 Munroe St là gì?

```
[Preamble: 192µs]
IEEE 802.11 Beacon frame, Flags: .....C
Type/Subtype: Beacon frame (0x0008)
Frame Control Field: 0x0000
.....00 = Version: 0
.....00.. = Type: Management frame (0)
1000..... = Subtype: 8
Flags: 0x00
.....00 = DS status: Not leaving DS or network is operating in AD-HOC mode (To DS: 0 From DS: 0)
.....0... = More Fragments: This is the last fragment
.....0... = Retry: Frame is not being retransmitted
.....0... = PWR MGT: STA will stay up
.....0... = More Data: No data buffered
.....0... = Protected flag: Data is not protected
.....0... = +HTC/Order flag: Not strictly ordered
.....0000 0000 0000 = Duration: 0 microseconds
Receiver address: Broadcast (ff:ff:ff:ff:ff:ff)
.....1..... = LG bit: Locally administered address (this is NOT the factory default)
.....1..... = IG bit: Group address (multicast/broadcast)
Destination address: Broadcast (ff:ff:ff:ff:ff:ff)
.....1..... = LG bit: Locally administered address (this is NOT the factory default)
.....1..... = IG bit: Group address (multicast/broadcast)
Transmitter address: CiscoLinksys_f7:1d:51 (00:16:b6:f7:1d:51)
.....0..... = LG bit: Globally unique address (factory default)
.....0..... = IG bit: Individual address (unicast)
Source address: CiscoLinksys_f7:1d:51 (00:16:b6:f7:1d:51)
.....0..... = LG bit: Globally unique address (factory default)
.....0..... = IG bit: Individual address (unicast)
BSS Id: CiscoLinksys_f7:1d:51 (00:16:b6:f7:1d:51)
.....0..... = LG bit: Globally unique address (factory default)
.....0..... = IG bit: Individual address (unicast)
.....0000 = Fragment number: 0
1011 0010 0110..... = Sequence number: 2854
Frame check sequence: 0x057e2608 [unverified]
[FCS Status: Unverified]
[MLAN Flags: .....C]
```

Đối với "30 Munroe St", BSS ID giống với địa chỉ MAC nguồn (ciscoLinksys\_f7:1d:51).

**Câu 6:** Các khung beacon từ điểm truy cập 30 Munroe St không quảng bá rằng điểm truy cập có thể hỗ trợ các mức tốc độ dữ liệu cao hơn và không có mục “tốc độ hỗ trợ mở rộng”. Các mức tốc độ đó là bao nhiêu?

```
..... = Reserved: 0
Tagged parameters (119 bytes)
Tag: SSID parameter set: "30 Munroe St"
Tag Number: SSID parameter set (0)
Tag length: 12
SSID: "30 Munroe St"

Tag: Supported Rates 1(B), 2(B), 5.5(B), 11(B), [Mbit/sec]
Tag Number: Supported Rates (1)
Tag length: 4
Supported Rates: 1(B) (0x82)
Supported Rates: 2(B) (0x84)
Supported Rates: 5.5(B) (0x8b)
Supported Rates: 11(B) (0x96)
```

Điểm truy cập "30 Munroe St" hỗ trợ các tốc độ dữ liệu sau:

- Supported Rates: 1 Mbps, 2 Mbps, 5.5 Mbps, và 11 Mbps.

Các tốc độ này được liệt kê trong phần "Tagged parameters" của khung beacon. Cụ thể:

- Tag: Supported Rates bao gồm:
  - 1(B) tương đương với 1 Mbps
  - 2(B) tương đương với 2 Mbps
  - 5.5(B) tương đương với 5.5 Mbps
  - 11(B) tương đương với 11 Mbps



### 3. Data Transfer

Vì bản vết (trace) bắt đầu khi máy trạm đã liên kết với điểm truy cập (AP), trước tiên hãy xem xét việc truyền dữ liệu qua một liên kết 802.11 trước khi xem xét liên kết/bỏ liên kết của AP. Nhớ rằng trong bản vết này, tại  $t=24.82t = 24.82t=24.82$ , máy trạm gửi yêu cầu HTTP đến <http://gaia.cs.umass.edu/wireshark-labs/alice.txt>. Địa chỉ IP của gaia.cs.umass.edu là 128.119.245.12. Sau đó, tại  $t=32.82t = 32.82t=32.82$ , máy trạm gửi yêu cầu HTTP đến <http://www.cs.umass.edu>.

**Câu hỏi 7:** Tìm khung 802.11 chứa đoạn SYN TCP đầu tiên trong phiên TCP này (tải xuống alice.txt). Ba địa chỉ MAC nào xuất hiện trong trường 802.11? Địa chỉ MAC nào trong khung này tương ứng với máy trạm không dây (hãy cung cấp địa chỉ MAC theo hệ thập lục phân của máy trạm)? Với điểm truy cập? Với bộ định tuyến nhảy đầu tiên? Địa chỉ IP của máy trạm không dây nào đang gửi đoạn SYN TCP này? Địa chỉ IP đích là gì? Địa chỉ đích này thuộc về máy trạm, điểm truy cập, bộ định tuyến nhảy đầu tiên, hay một thiết bị khác trên mạng? Hãy giải thích.

Sử dụng bộ lọc tcp.flags.syn == 1 trong Wireshark để lọc và chỉ hiển thị các gói tin SYN. Bộ lọc này sẽ giúp bạn tìm các gói tin bắt đầu một phiên TCP mới.

Wireshark\_802.11.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tcp.flags.syn == 1

No.	Time	Source	Destination	Protocol	Length	Info
474	09:05:31.883550	192.168.1.109	128.119.245.12	TCP	110	2538 → 80 [SYN] Seq=0 Win=16384 Len=0 MSS=1460 SACK_PERM
476	09:05:31.900208	128.119.245.12	192.168.1.109	TCP	110	80 → 2538 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 SACK_PERM
1011	09:05:39.881031	192.168.1.109	128.119.240.19	TCP	110	2541 → 80 [SYN] Seq=0 Win=16384 Len=0 MSS=1460 SACK_PERM
1013	09:05:39.898088	128.119.240.19	192.168.1.109	TCP	110	80 → 2541 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460 SACK_PERM
1034	09:05:39.941719	192.168.1.109	128.119.240.19	TCP	110	2542 → 80 [SYN] Seq=0 Win=16384 Len=0 MSS=1460 SACK_PERM
1047	09:05:39.963357	128.119.240.19	192.168.1.109	TCP	110	80 → 2542 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460 SACK_PERM
1048	09:05:39.963455	128.119.240.19	192.168.1.109	TCP	110	[TCP Retransmission] 80 → 2542 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460 SACK_PERM
1051	09:05:39.963993	128.119.240.19	192.168.1.109	TCP	110	[TCP Retransmission] 80 → 2542 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460 SACK_PERM
1058	09:05:39.975642	128.119.101.5	192.168.1.109	TCP	110	80 → 2543 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460 SACK_PERM
1119	09:05:40.029664	192.168.1.109	128.119.240.19	TCP	110	2544 → 80 [SYN] Seq=0 Win=16384 Len=0 MSS=1460 SACK_PERM
1121	09:05:40.030655	192.168.1.109	128.119.240.19	TCP	110	2545 → 80 [SYN] Seq=0 Win=16384 Len=0 MSS=1460 SACK_PERM
1130	09:05:40.051164	128.119.240.19	192.168.1.109	TCP	110	80 → 2544 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460 SACK_PERM
1134	09:05:40.051617	128.119.240.19	192.168.1.109	TCP	110	80 → 2545 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460 SACK_PERM
1142	09:05:40.054406	192.168.1.109	64.233.187.104	TCP	110	2546 → 80 [SYN] Seq=0 Win=16384 Len=0 MSS=1460 SACK_PERM
1143	09:05:40.054772	192.168.1.109	64.233.187.104	TCP	110	[TCP Retransmission] 2546 → 80 [SYN] Seq=0 Win=16384 Len=0 MSS=1460 SACK_PERM
1153	09:05:40.074032	192.168.1.109	128.119.240.19	TCP	110	2547 → 80 [SYN] Seq=0 Win=16384 Len=0 MSS=1460 SACK_PERM
1165	09:05:40.094204	128.119.240.19	192.168.1.109	TCP	110	80 → 2547 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460 SACK_PERM
1177	09:05:40.102960	64.233.187.104	192.168.1.109	TCP	108	80 → 2546 [SYN, ACK] Seq=0 Ack=1 Win=8190 Len=0 MSS=1460
1262	09:05:40.171520	192.168.1.109	128.119.240.19	TCP	110	2548 → 80 [SYN] Seq=0 Win=16384 Len=0 MSS=1460 SACK_PERM
1280	09:05:40.187665	192.168.1.109	128.119.240.19	TCP	110	2549 → 80 [SYN] Seq=0 Win=16384 Len=0 MSS=1460 SACK_PERM
1284	09:05:40.194126	128.119.240.19	192.168.1.109	TCP	110	80 → 2548 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460 SACK_PERM
1285	09:05:40.194260	128.119.240.19	192.168.1.109	TCP	110	[TCP Retransmission] 80 → 2548 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460 SACK_PERM
1300	09:05:40.212086	128.119.240.19	192.168.1.109	TCP	110	80 → 2549 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460 SACK_PERM
1714	09:05:56.092813	128.119.101.5	192.168.1.109	TCP	108	80 → 2543 [SYN, PSH, ECE, AE] Seq=0 Win=7504[Malformed Packet]

Ba địa chỉ MAC trong khung 802.11 (gói tin SYN TCP đầu tiên):



- Receiver Address (địa chỉ nhận): 00:16:b6:f7:1d:51 (CiscoLinksys\_f7:1d:51) – địa chỉ MAC của điểm truy cập.
- Transmitter Address (địa chỉ truyền): 00:13:02:d1:b6:4f (Intel\_d1:b6:4f) – địa chỉ MAC của máy trạm không dây.
- BSSID: 00:16:b6:f7:1d:51 (CiscoLinksys\_f7:1d:51) – cũng là địa chỉ MAC của điểm truy cập.

Xác định địa chỉ MAC của từng thiết bị:

- Địa chỉ MAC của máy trạm không dây: 00:13:02:d1:b6:4f (Intel\_d1:b6:4f)
- Địa chỉ MAC của điểm truy cập (AP): 00:16:b6:f7:1d:51 (CiscoLinksys\_f7:1d:51)
- Bộ định tuyến nhảy đầu tiên: Địa chỉ MAC của bộ định tuyến nhảy đầu tiên không xuất hiện trong khung 802.11 này. Thay vào đó, địa chỉ này sẽ xuất hiện trong gói tin khi nó đi qua mạng có dây sau điểm truy cập.

Địa chỉ IP của máy trạm không dây gửi đoạn SYN TCP: 192.168.1.109

Địa chỉ IP đích: 128.119.245.12

```
IEEE 802.11 QoS Data, Flags: .....TC
Type/Subtype: QoS Data (0x0028)
Frame Control Field: 0x8801
....00 = Version: 0
....10.. = Type: Data frame (2)
1000.... = Subtype: 8
Flags: 0x01
....01 = DS status: Frame from STA to DS via an AP (To DS: 1 From DS: 0) (0x1)
....0... = More Fragments: This is the last fragment
....0... = Retry: Frame is not being retransmitted
...0.... = PWR MGT: STA will stay up
..0.... = More Data: No data buffered
.0... = Protected flag: Data is not protected
0... = +HTC/Order flag: Not strictly ordered
.000 0000 0010 1100 = Duration: 44 microseconds
Receiver address: CiscoLinksys_f7:1d:51 (00:16:b6:f7:1d:51)
....0... = LG bit: Globally unique address (factory default)
....0... = IG bit: Individual address (unicast)
Transmitter address: Intel_d1:b6:4f (00:13:02:d1:b6:4f)
....0... = LG bit: Globally unique address (factory default)
....0... = IG bit: Individual address (unicast)
Destination address: CiscoLinksys_f4:eb:a8 (00:16:b6:f4:eb:a8)
....0... = LG bit: Globally unique address (factory default)
....0... = IG bit: Individual address (unicast)
Source address: Intel_d1:b6:4f (00:13:02:d1:b6:4f)
....0... = LG bit: Globally unique address (factory default)
....0... = IG bit: Individual address (unicast)
BSS Id: CiscoLinksys_f7:1d:51 (00:16:b6:f7:1d:51)
....0... = LG bit: Globally unique address (factory default)
....0... = IG bit: Individual address (unicast)
STA address: Intel_d1:b6:4f (00:13:02:d1:b6:4f)
....0... = LG bit: Globally unique address (factory default)
....0... = IG bit: Individual address (unicast)
....0000 = Fragment number: 0
0000 0011 0001 .... = Sequence number: 49
```

Giải thích: Địa chỉ IP đích 128.119.245.12 là địa chỉ của máy chủ từ xa (gaia.cs.umass.edu) nơi chứa tệp alice.txt, không phải là địa chỉ của máy trạm, điểm truy cập hoặc bộ định tuyến nhảy đầu tiên. Máy trạm không dây đang gửi yêu cầu đến một máy chủ bên ngoài qua Internet, và điểm truy cập đóng vai trò là cầu nối để truyền dữ liệu đến bộ định tuyến và ra ngoài mạng.

**Câu hỏi 8:** Tìm khung 802.11 chứa đoạn SYN-ACK cho phiên TCP này. Ba địa chỉ MAC nào xuất hiện trong trường 802.11? Địa chỉ MAC nào trong khung này tương ứng với máy trạm? Với điểm truy cập? Với bộ định tuyến nhảy đầu tiên? Địa chỉ MAC người gửi trong khung có tương ứng với địa chỉ IP của thiết bị đã gửi đoạn TCP SYN-ACK trong gói dữ liệu này không? (Gợi ý: Xem lại Hình 6.19 trong sách nếu bạn không chắc cách trả lời câu hỏi này hoặc tham khảo phản tương ứng của câu hỏi trước đó. Điều này đặc biệt quan trọng để bạn hiểu được.)

Sử dụng bộ lọc `tcp.flags.syn == 1 && tcp.flags.ack == 1` trong Wireshark để chỉ hiển thị các gói tin SYN-ACK.

Sau khi lọc, tìm gói tin SYN-ACK mà trong đó Destination IP Address trùng với Source IP Address của gói tin SYN đã tìm thấy ở câu 7. Đây là gói tin phản hồi từ máy chủ cho yêu cầu TCP ban đầu từ máy khách.

Ba địa chỉ MAC trong khung 802.11 (gói tin SYN-ACK):

- Receiver Address (địa chỉ nhận): 00:13:02:d1:b6:4f (Intel\_d1:b6:4f) – địa chỉ MAC của máy trạm không dây.
- Transmitter Address (địa chỉ truyền): 00:16:b6:f7:1d:51 (CiscoLinksys\_f7:1d:51) – địa chỉ MAC của điểm truy cập.
- BSSID: 00:16:b6:f7:1d:51 (CiscoLinksys\_f7:1d:51) – cũng là địa chỉ MAC của điểm truy cập.

Xác định địa chỉ MAC của từng thiết bị:

- Địa chỉ MAC của máy trạm không dây: 00:13:02:d1:b6:4f (Intel\_d1:b6:4f)
- Địa chỉ MAC của điểm truy cập (AP): 00:16:b6:f7:1d:51 (CiscoLinksys\_f7:1d:51)

- Bộ định tuyến nhảy đầu tiên: Địa chỉ MAC của bộ định tuyến nhảy đầu tiên không xuất hiện trong khung 802.11 này. Địa chỉ này sẽ xuất hiện trong các gói tin mạng có dây khi gói tin rời khỏi mạng WiFi.

```
IEEE 802.11 QoS Data, Flags: ..mP..F.C
Type/Subtype: QoS Data (0x0028)
Frame Control Field: 0x8832
.... ..00 = Version: 0
.... 10.. = Type: Data frame (2)
1000 .... = Subtype: 8
Flags: 0x32
.... ..10 = DS status: Frame from DS to a STA via AP(To DS: 0 From DS: 1) (0x2)
.... .0.. = More Fragments: This is the last fragment
.... 0... = Retry: Frame is not being retransmitted
.... 1... = PWR MGT: STA will go to sleep
..1. .... = More Data: Data is buffered for STA at AP
.0.. .... = Protected flag: Data is not protected
0... .... = +HTC/Order flag: Not strictly ordered
Duration/ID: 11560 (reserved)
Receiver address: 91:2a:b0:49:b6:4f (91:2a:b0:49:b6:4f)
.... ..0. .... = LG bit: Globally unique address (factory default)
.... ...1 .... = IG bit: Group address (multicast/broadcast)
Transmitter address: CiscoLinksys_f7:1d:51 (00:16:b6:f7:1d:51)
.... ..0. .... = LG bit: Globally unique address (factory default)
.... ...0 .... = IG bit: Individual address (unicast)
Destination address: 91:2a:b0:49:b6:4f (91:2a:b0:49:b6:4f)
.... ..0. .... = LG bit: Globally unique address (factory default)
.... ...1 .... = IG bit: Group address (multicast/broadcast)
Source address: CiscoLinksys_f4:eb:a8 (00:16:b6:f4:eb:a8)
.... ..0. .... = LG bit: Globally unique address (factory default)
.... ...0 .... = IG bit: Individual address (unicast)
BSS Id: CiscoLinksys_f7:1d:51 (00:16:b6:f7:1d:51)
.... ..0. .... = LG bit: Globally unique address (factory default)
.... ...0 .... = IG bit: Individual address (unicast)
STA address: 91:2a:b0:49:b6:4f (91:2a:b0:49:b6:4f)
.... ..0. .... = LG bit: Globally unique address (factory default)
.... ...1 .... = IG bit: Group address (multicast/broadcast)
.... .... 0000 = Fragment number: 0
1100 0011 0100 .... = Sequence number: 3124
Frame check sequence: 0xecdc407d [unverified]
[FCS Status: Unverified]
[WLAN Flags: ..mP..F.C]
```

Địa chỉ MAC của người gửi trong khung có tương ứng với địa chỉ IP đã gửi TCP SYN-ACK không? Có. Địa chỉ MAC của người gửi (Transmitter Address) trong khung này là của điểm truy cập 00:16:b6:f7:1d:51, nhưng trên thực tế, nó đại diện cho việc truyền lại từ máy chủ trên mạng có dây. Vì vậy, địa chỉ MAC này không phải là địa chỉ MAC thực của máy chủ, mà là của điểm truy cập đã chuyển tiếp gói tin SYN-ACK từ mạng có dây sang mạng không dây để gửi đến máy trạm.

#### 4. Association/Disassociation

Nhớ lại từ Phần 7.3.1 trong sách rằng máy trạm phải liên kết (associate) với một điểm truy cập trước khi gửi dữ liệu. Việc liên kết trong 802.11 được thực hiện bằng cách sử dụng khung ASSOCIATE REQUEST (gửi từ máy trạm đến AP, với loại khung là 0 và loại phụ là 0, xem Phần 7.3.3 trong sách) và khung ASSOCIATE RESPONSE (gửi từ AP đến máy trạm với loại khung là 0 và loại phụ là 1, để phản hồi yêu cầu liên kết ASSOCIATE REQUEST). Để có lời giải thích chi tiết về mỗi trường trong khung 802.11, xem trang 34 (Phần 7) của đặc tả IEEE 802.11 tại <http://gaia.cs.umass.edu/wireshark-labs/802.11-1999.pdf>.

**Câu hỏi 9:** Hai hành động nào (ví dụ: các khung nào được gửi) mà máy trạm thực hiện trong bản vết ngay sau  $t=49t=49$ , để kết thúc liên kết với điểm truy cập "30 Munroe St" mà ban đầu đã được thiết lập khi quá trình thu thập bản vết bắt đầu? (Gợi ý: một là hành động ở lớp IP, và một là hành động ở lớp 802.11). Khi xem đặc tả 802.11, có hành động nào khác mà bạn có thể đã mong đợi thấy nhưng lại không có ở đây không?

```
Signal/noise ratio (dB): 73 dB
[Duration: 28µs]
[Preamble: 20µs]
IEEE 802.11 Deauthentication, Flags: .....C
Type/Subtype: Deauthentication (0x000c)
Frame Control Field: 0xc000
....0000 = Version: 0
....0000 = Type: Management frame (0)
1100.... = Subtype: 12
Flags: 0x00
....0000 = DS status: Not leaving DS or network is operating in AD-HOC mode (To DS: 0 From DS: 0) (0x0)
....0000 = More Fragments: This is the last fragment
....0000 = Retry: Frame is not being retransmitted
..0000 = PWR MGT: STA will stay up
..0000 = More Data: No data buffered
..0000 = Protected flag: Data is not protected
0000.... = +HTC/Order flag: Not strictly ordered
.000000001100 = Duration: 44 microseconds
Receiver address: CiscoLinksys_f7:1d:51 (00:16:b6:f7:1d:51)
....0000.... = LG bit: Globally unique address (factory default)
....0000.... = IG bit: Individual address (unicast)
Destination address: CiscoLinksys_f7:1d:51 (00:16:b6:f7:1d:51)
....0000.... = LG bit: Globally unique address (factory default)
....0000.... = IG bit: Individual address (unicast)
Transmitter address: Intel_d1:b6:4f (00:13:02:d1:b6:4f)
....0000.... = LG bit: Globally unique address (factory default)
....0000.... = IG bit: Individual address (unicast)
Source address: Intel_d1:b6:4f (00:13:02:d1:b6:4f)
....0000.... = LG bit: Globally unique address (factory default)
....0000.... = IG bit: Individual address (unicast)
BSS Id: CiscoLinksys_f7:1d:51 (00:16:b6:f7:1d:51)
....0000.... = LG bit: Globally unique address (factory default)
....0000.... = IG bit: Individual address (unicast)
....0000 = Fragment number: 0
011001000101.... = Sequence number: 1605
Frame check sequence: 0x3b4a8b9c [unverified]
[FCS Status: Unverified]
[WLAN Flags: .....C]
IEEE 802.11 Wireless Management
Fixed parameters (2 bytes)
Reason code: Unspecified reason (0x0001)
```

Hành động ở lớp 802.11: Máy trạm gửi một gói tin Deauthentication đến điểm truy cập 30 Munroe St để thông báo về việc ngắt kết nối. Gói tin này xuất hiện trong Frame 1735 với các chi tiết sau:

- Source (Transmitter) Address: Intel\_d1:b6:4f (địa chỉ MAC của máy trạm).
- Destination (Receiver) Address: CiscoLinksys\_f7:1d:51 (địa chỉ MAC của điểm truy cập).
- BSSID: CiscoLinksys\_f7:1d:51.
- Reason Code: 1 (Unspecified reason).

Hành động ở lớp IP: Không có gói tin FIN hoặc RST được tìm thấy ngay sau  $t = 49$  trong dấu vết để chỉ ra hành động ngắt kết nối ở lớp IP. Máy trạm thực hiện việc ngắt kết nối ở lớp 802.11 thông qua gói tin Deauthentication mà không cần hành động lớp IP bổ sung.

**Câu hỏi 10:** Kiểm tra bản vết và tìm các khung AUTHENTICATION gửi từ máy trạm đến AP và ngược lại. Có bao nhiêu tin nhắn AUTHENTICATION được gửi từ máy trạm không dây đến linksys\_ses\_24086 AP (có địa chỉ MAC là Cisco\_Li\_f5:ba:bb) bắt đầu vào khoảng  $t=49t = 49t=49$ ?

Wireshark\_802.11.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

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

No.	Time	Source	Destination	Protocol	Length	Info
1740	09:05:56.711314	Intel_d1:b6:4f	CiscoLinksys_f5:ba:...	802.11	58	Authentication, SN=1606, FN=0, Flags=.....C
1741	09:05:56.712157	Intel_d1:b6:4f	CiscoLinksys_f5:ba:...	802.11	58	Authentication, SN=1606, FN=0, Flags=....R...C
1742	09:05:56.713159	Intel_d1:b6:4f	CiscoLinksys_f5:ba:...	802.11	58	Authentication, SN=1606, FN=0, Flags=....R...C
1744	09:05:56.714772	Intel_d1:b6:4f	CiscoLinksys_f5:ba:...	802.11	58	Authentication, SN=1606, FN=0, Flags=....R...C
1746	09:05:56.717776	Intel_d1:b6:4f	CiscoLinksys_f5:ba:...	802.11	58	Authentication, SN=1606, FN=0, Flags=....R...C
1749	09:05:56.722162	Intel_d1:b6:4f	CiscoLinksys_f5:ba:...	802.11	58	Authentication, SN=1606, FN=0, Flags=....R...C
1821	09:06:00.858290	Intel_d1:b6:4f	CiscoLinksys_f5:ba:...	802.11	58	Authentication, SN=1612, FN=0, Flags=.....C
1822	09:06:00.859527	Intel_d1:b6:4f	CiscoLinksys_f5:ba:...	802.11	58	Authentication, SN=1612, FN=0, Flags=....R...C
1921	09:06:04.961689	Intel_d1:b6:4f	CiscoLinksys_f5:ba:...	802.11	58	Authentication, SN=1619, FN=0, Flags=.....C
1922	09:06:04.962782	Intel_d1:b6:4f	CiscoLinksys_f5:ba:...	802.11	58	Authentication, SN=1619, FN=0, Flags=....R...C
1923	09:06:04.963778	Intel_d1:b6:4f	CiscoLinksys_f5:ba:...	802.11	58	Authentication, SN=1619, FN=0, Flags=....R...C
1924	09:06:04.969427	Intel_d1:b6:4f	CiscoLinksys_f5:ba:...	802.11	58	Authentication, SN=1619, FN=0, Flags=....R...C
2122	09:06:09.244408	Intel_d1:b6:4f	CiscoLinksys_f5:ba:...	802.11	58	Authentication, SN=1644, FN=0, Flags=.....C
2123	09:06:09.245403	Intel_d1:b6:4f	CiscoLinksys_f5:ba:...	802.11	58	Authentication, SN=1644, FN=0, Flags=....R...C
2124	09:06:09.246527	Intel_d1:b6:4f	CiscoLinksys_f5:ba:...	802.11	58	Authentication, SN=1644, FN=0, Flags=....R...C
2156	09:06:10.240544	Intel_d1:b6:4f	CiscoLinksys_f7:1d:...	802.11	58	Authentication, SN=1647, FN=0, Flags=.....C
2158	09:06:10.241528	CiscoLinksys_f7:1d:...	Intel_d1:b6:4f	802.11	58	Authentication, SN=3726, FN=0, Flags=.....C
2160	09:06:10.242164	Intel_d1:b6:4f	CiscoLinksys_f7:1d:...	802.11	58	Authentication, SN=1647, FN=0, Flags=....R...C
2164	09:06:10.243149	CiscoLinksys_f7:1d:...	Intel_d1:b6:4f	802.11	58	Authentication, SN=3727, FN=0, Flags=.....C

Máy trạm (địa chỉ MAC Intel\_d1:b6:4f) gửi nhiều khung Authentication đến điểm truy cập linksys\_ses\_24086 (địa chỉ MAC Cisco\_Li\_f5:ba:bb).

Tổng cộng, có 4 khung Authentication được gửi từ máy trạm đến điểm truy cập linksys\_ses\_24086.

Các khung Authentication này có thể được tìm thấy trong dấu vết với các chi tiết sau:

- Source Address: Intel\_d1:b6:4f (địa chỉ MAC của máy trạm).
- Destination Address: Cisco\_Li\_f5:ba:bb (địa chỉ MAC của điểm truy cập linksys\_ses\_24086).
- Tất cả các khung đều có Authentication Algorithm là Open System (không yêu cầu khóa).

**Câu hỏi 11:** Máy trạm có muốn xác thực yêu cầu một khóa hay mở không?

```
.... .... 0000 = Fragment number: 0
1110 1000 1110 .... = Sequence number: 3726
Frame check sequence: 0x93eae9c9 [unverified]
[FCS Status: Unverified]
[WLAN Flags: .....C]
IEEE 802.11 Wireless Management
Fixed parameters (6 bytes)
  Authentication Algorithm: Open System (0)
  Authentication SEQ: 0x0002
  Status code: Successful (0x0000)
```

Máy trạm sử dụng Open System cho quá trình xác thực, điều này có nghĩa là không yêu cầu khóa. Điều này có thể được xác định từ trường Authentication Algorithm trong khung Authentication của máy trạm.

**Câu hỏi 12:** Bạn có thấy bất kỳ khung AUTHENTICATION nào từ linksys\_ses\_24086 AP trong bản vết không?

```
Frame 2158: 58 bytes on wire (464 bits), 58 bytes captured (464 bits)
Encapsulation type: IEEE 802.11 plus radiotap radio header (23)
Arrival Time: Jun 29, 2007 09:06:10.241528000 SE Asia Standard Time
UTC Arrival Time: Jun 29, 2007 02:06:10.241528000 UTC
Epoch Arrival Time: 1183882770.241528000
[Time shift for this packet: 0.000000000 seconds]
[Time delta from previous captured frame: 0.000849000 seconds]
[Time delta from previous displayed frame: 0.000984000 seconds]
[Time since reference or first frame: 63.169071000 seconds]
Frame Number: 2158
Frame Length: 58 bytes (464 bits)
Capture Length: 58 bytes (464 bits)
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: radiotap:wlan_radio:wlan]
Radiotap Header v0, Length 24
Header revision: 0
Header pad: 0
Header length: 24
Present flags
  Present flags word: 0x000058ee
```



Có một khung Authentication từ điểm truy cập linksys\_ses\_24086 đến máy trạm. Khung này có Source Address là địa chỉ MAC của linksys\_ses\_24086 và Destination Address là địa chỉ MAC của máy trạm.

**Câu hỏi 13:** Bây giờ hãy xem xét điều gì sẽ xảy ra khi máy trạm từ bỏ việc cố gắng liên kết với linksys\_ses\_24086 AP và bây giờ cố gắng liên kết lại với "30 Munroe St" AP. Tìm các khung AUTHENTICATION gửi từ máy trạm đến AP và ngược lại. Tại những thời điểm nào có một khung AUTHENTICATION từ máy trạm đến "30 Munroe St" AP, và khi nào thì có khung AUTHENTICATION gửi từ AP đến máy trạm trong phản hồi? (Lưu ý rằng bạn có thể sử dụng biểu thức lọc wlan.fc.subtype == 11 and wlan.fc.type == 0 and wlan.addr == IntelCor\_d1:b6:4f để chỉ hiển thị các khung AUTHENTICATION trong bản vết này cho máy trạm không dây.)

Máy trạm gửi khung **Authentication** đến AP **"30 Munroe St"** tại thời điểm 09:06:10.241528. AP **"30 Munroe St"** gửi lại phản hồi **Authentication** đến máy trạm tại thời điểm 09:06:10.264558.

```
3310E 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
```

**Câu hỏi 14:** Một ASSOCIATE REQUEST từ máy trạm đến AP, và một phản hồi ASSOCIATE RESPONSE từ AP đến máy trạm được sử dụng cho quá trình liên kết với một AP. Tại thời điểm nào có một ASSOCIATE REQUEST từ máy trạm đến "30 Munroe St" AP? Khi nào thì phản hồi ASSOCIATE REPLY được gửi? (Lưu ý rằng bạn có thể sử dụng biểu thức lọc wlan.fc.subtype < 2 and wlan.fc.type == 0 and wlan.addr == IntelCor\_d1:b6:4f để chỉ hiển thị các khung ASSOCIATE REQUEST và ASSOCIATE RESPONSE cho bản vết này).

```
3310E 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
```



Máy trạm gửi khung Associate Request đến AP "30 Munroe St" tại thời điểm 09:06:10.242367. AP "30 Munroe St" gửi lại phản hồi Associate Response đến máy trạm tại thời điểm 09:06:10.264558.

**Câu hỏi 15:** Tốc độ truyền mà máy trạm sẵn sàng sử dụng là gì? AP thì sao? Để trả lời câu hỏi này, bạn sẽ cần tìm trong các trường thông số của khung quản lý mạng LAN không dây 802.11.

Máy trạm sẵn sàng sử dụng các tốc độ truyền: 1, 2, 5.5, và 11 Mbps (từ trường Supported Rates trong khung Associate Request). AP "30 Munroe St" hỗ trợ các tốc độ truyền thêm: 6, 9, 12, 18, 24, 36, 48, và 54 Mbps (từ trường Extended Supported Rates trong khung Beacon).

### **5. Other Frame types**

Trace chứa một số khung PROBE REQUEST và PROBE RESPONSE.

**Câu hỏi 16:** Địa chỉ MAC của người gửi, người nhận và BSS ID trong các khung này là gì? Mục đích của hai loại khung này là gì? (Để trả lời câu hỏi cuối cùng này, bạn sẽ cần tìm hiểu kỹ các tài liệu tham khảo trực tuyến được trích dẫn trước đó trong phòng thí nghiệm này)