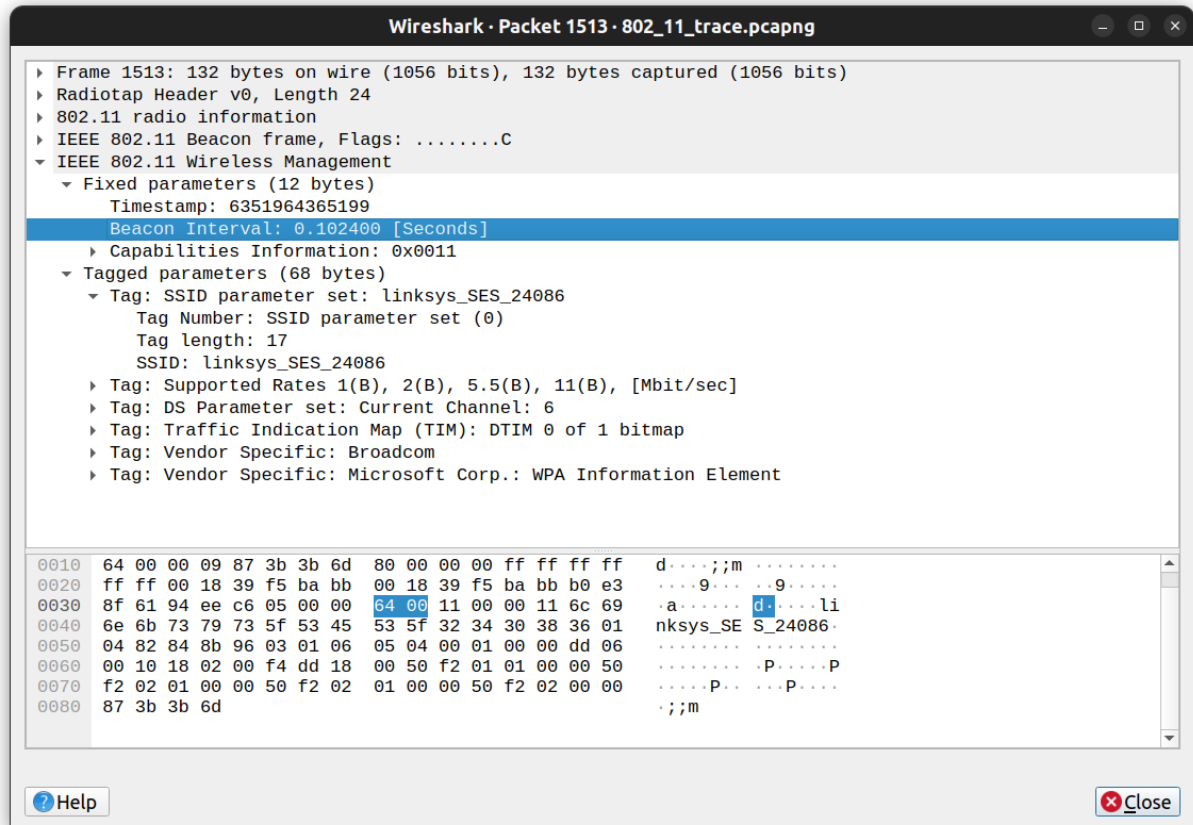
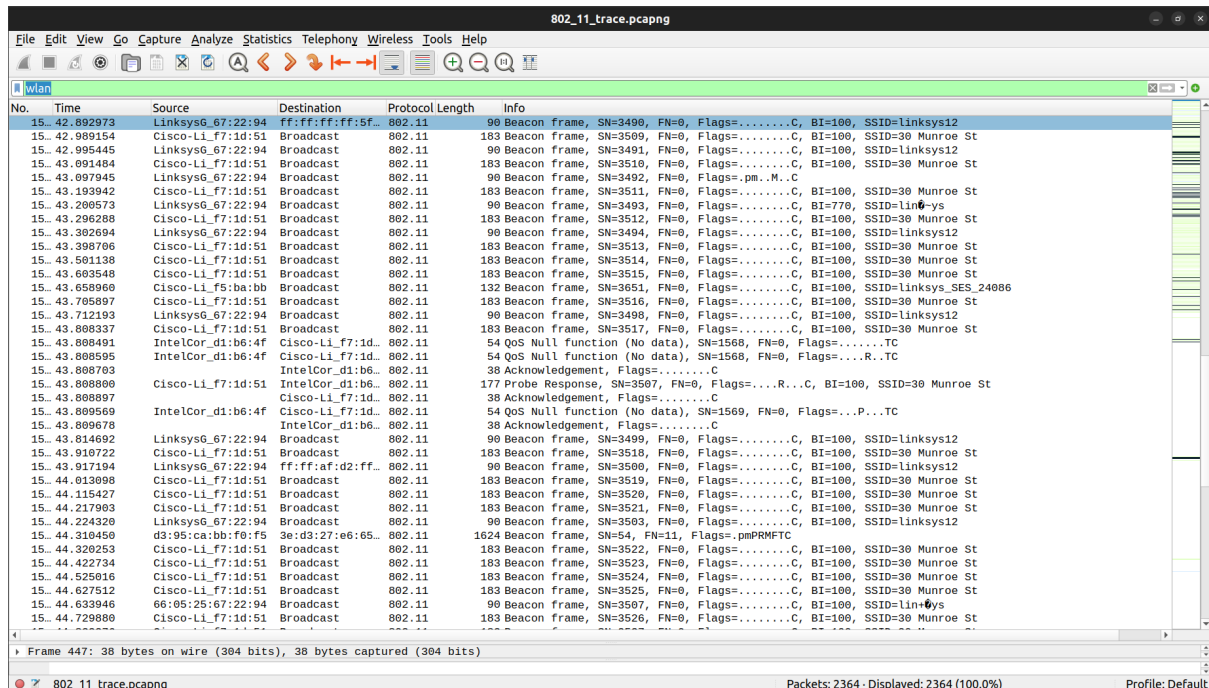
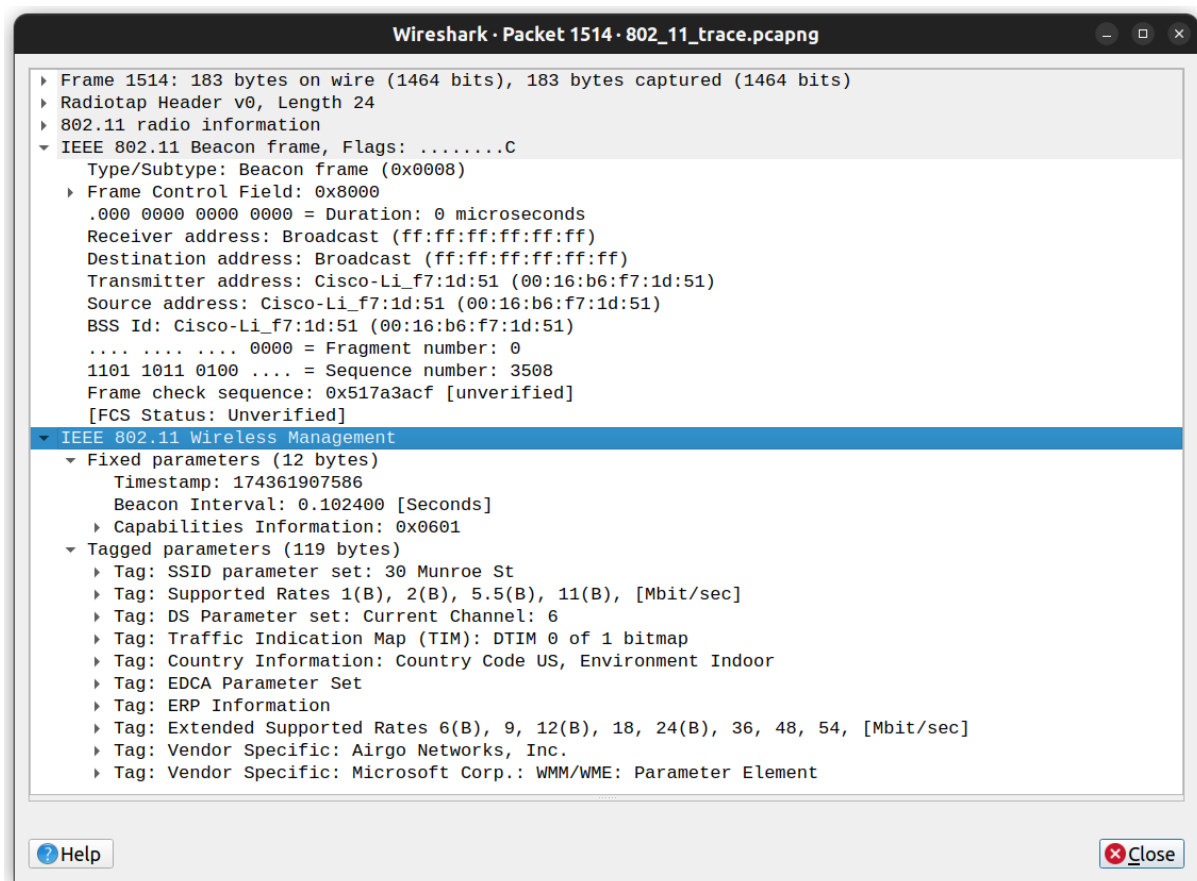


Маяковые кадры

Найдите кадры-маяки, используемые точкой доступа 802.11 для оповещения о своем существовании.





1. Каковы SSID двух точек доступа, которые выдают большинство кадров маяка в этой трассировке?

- SSID - 30 Munroe St
- SSID - linksys_SES_24086

2. Каковы интервалы времени между передачами кадров маяка в точке доступа *linksys_SES_24086*? С точки доступа *30 Munroe St*? (Подсказка: этот интервал времени содержится в самом кадре маяка).

- Beacon Interval для 30 Munroe St - 0,1024 секунд
- Beacon Interval для linksys_SES_24086 - 0,1024 секунд

3. Каков исходный MAC-адрес в кадре маяка *30 Munroe St*?

- Исходный MAC-адрес - 00:16:b6:f7:1d:51

4. Каков MAC-адрес назначения в кадре маяка *30 Munroe St*?

- MAC-адрес назначения - ff:ff:ff:ff:ff:ff (Broadcast)

5. Каков идентификатор MAC BSS в кадре маяка *30 Munroe St*?

- BSS ID - 00:16:b6:f7:1d:51

6. Кадры маяка с точки доступа *30 Munroe St*, рекламируют, что точка доступа может поддерживать 4 скорости передачи данных и 8 дополнительных “расширенных поддерживаемых скоростей”. Что это за скорости?

- *Supported Rates:* 1, 2, 5.5, 11 Мбит/с
- *Extended Supported Rates:* 6, 9, 12, 18, 24, 36, 48, 54 Мбит/с

Передача данных

Найдите кадр 802.11, содержащий сегмент SYN TCP для этого первого сеанса TCP (который загружает alice.txt)

The image shows a Wireshark packet capture titled "802_11_trace.pcapng". The interface displays a list of captured packets in the packet list pane, with details and packet bytes panes visible for the selected packet (Frame 474).

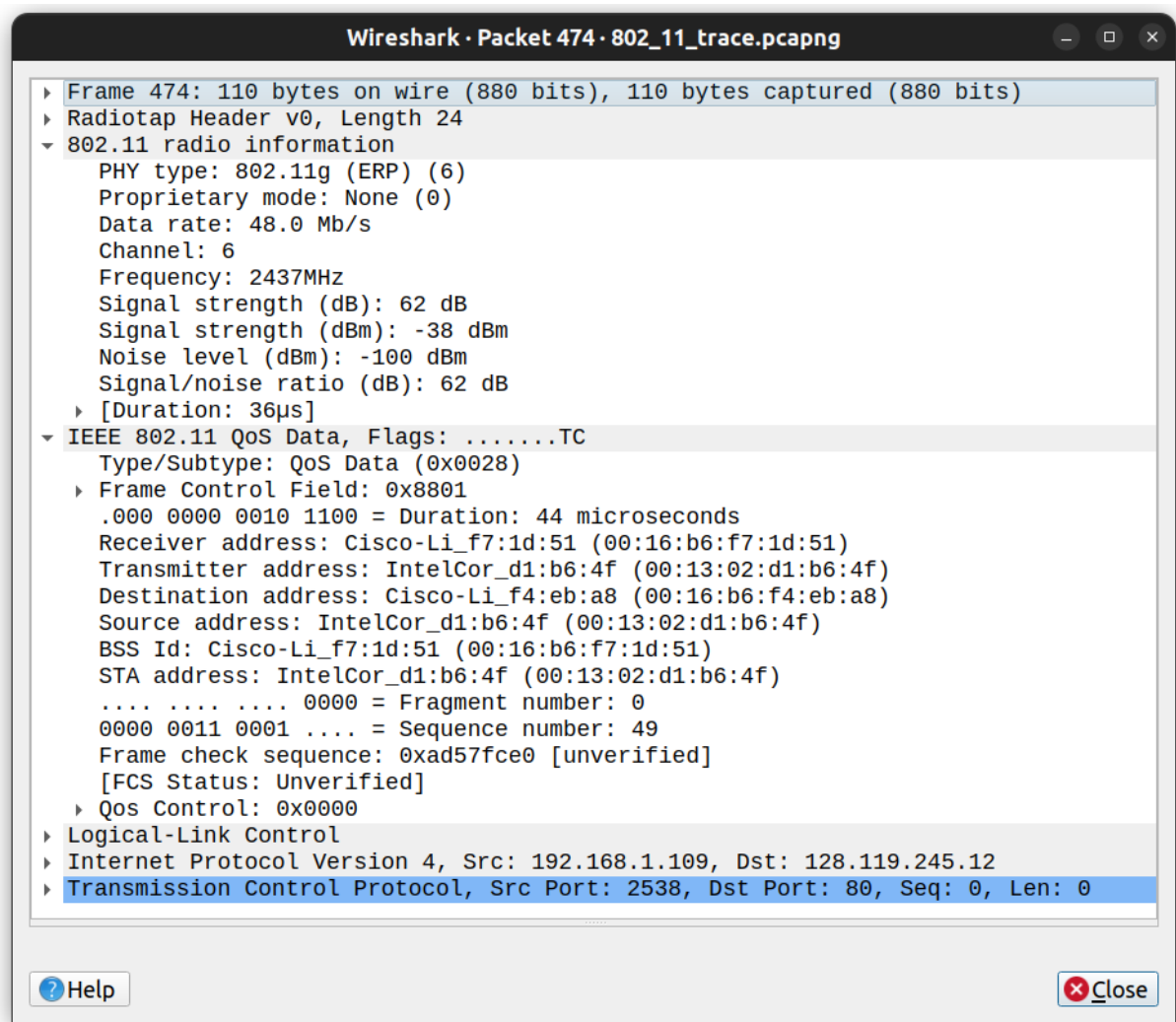
Packet List:

No.	Time	Source	Destination	Protocol	Length	Info
453	24.148410	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3114, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
454	24.250778	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3115, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
455	24.353107	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3116, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
456	24.455592	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3117, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
457	24.557988	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3118, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
458	24.660319	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3119, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
459	24.763182	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=3120, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
460	24.763316	IntelCor_d1:b6:4f	IntelCor_d1:b6:4f	802.11	38	Acknowledgement, Flags=.....C
461	24.763424	Cisco-Li_f7:1d:51	IntelCor_d1:b6:4f	802.11	177	Probe Response, SN=3121, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
462	24.763522	Cisco-Li_f7:1d:51	Cisco-Li_f7:1d:51	802.11	38	Acknowledgement, Flags=.....C
463	24.764328	IntelCor_d1:b6:4f	Cisco-Li_f7:1d:51	802.11	54	QoS Null function (No data), SN=1531, FN=0, Flags=...P...TC
464	24.764419	IntelCor_d1:b6:4f	IntelCor_d1:b6:4f	802.11	38	Acknowledgement, Flags=.....C
465	24.792352	IntelCor_d1:b6:4f	LLC	90	S P, func=RNR, N(R)=87; DSAP Banyan Vines Group, SSAP 0x6a Command	
466	24.792693	IntelCor_d1:b6:4f	Broadcast	ARP	90	Who has 192.168.1.1? Tell 192.168.1.109
467	24.792793	IntelCor_d1:b6:4f	IntelCor_d1:b6:4f	802.11	38	Acknowledgement, Flags=.....C
468	24.795431	Cisco-Li_f7:1d:51	Cisco-Li_f4:eb:..	802.11	90	Fragmented IEEE 802.11 frame
469	24.795573	Cisco-Li_f7:1d:51	Cisco-Li_f7:1d:51	802.11	38	Acknowledgement, Flags=.....C
470	24.795673	192.168.1.109	nrcns.chelmsfd..	DNS	125	Standard query 0x7892 A gaia.cs.umass.edu
471	24.795769	IntelCor_d1:b6:4f	IntelCor_d1:b6:4f	802.11	38	Acknowledgement, Flags=.....C
472	24.809325	nrcns.chelmsfd..	192.168.1.109	DNS	141	Standard query response 0x7892 A gaia.cs.umass.edu A 128.119.245.12
473	24.809513	Cisco-Li_f7:1d:51	Cisco-Li_f7:1d:51	802.11	38	Acknowledgement, Flags=.....C
474	24.811093	192.168.1.109	gaia.cs.umass..	TCP	110	vnwk-prapi(2538) -> http(80) [SYN] Seq=0 Win=16384 Len=0 MSS=1460 SACK_PERM=1
475	24.811231	IntelCor_d1:b6:4f	IntelCor_d1:b6:4f	802.11	38	Acknowledgement, Flags=.....C
476	24.827751	gaia.cs.umass.edu	192.168.1.109	TCP	110	http(80) -> vnwk-prapi(2538) [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 SACK_PERM=1
477	24.827922	Cisco-Li_f7:1d:51	Cisco-Li_f7:1d:51	802.11	38	Acknowledgement, Flags=.....C
478	24.828024	gaia.cs.umass..	192.168.1.109	TCP	102	vnwk-prapi(2538) -> http(80) [ACK] Seq=1 Ack=1 Win=17520 Len=0
479	24.828148	IntelCor_d1:b6:4f	IntelCor_d1:b6:4f	802.11	38	Acknowledgement, Flags=.....C
480	24.828253	192.168.1.109	gaia.cs.umass..	HTTP	537	GET /wreshark-labs/alice.txt HTTP/1.1
481	24.828352	IntelCor_d1:b6:4f	IntelCor_d1:b6:4f	802.11	38	Acknowledgement, Flags=.....C
482	24.846898	gaia.cs.umass.edu	192.168.1.109	TCP	108	http(80) -> vnwk-prapi(2538) [ACK] Seq=1 Ack=436 Win=6432 Len=0
483	24.847058	Cisco-Li_f7:1d:51	Cisco-Li_f7:1d:51	802.11	38	Acknowledgement, Flags=.....C
484	24.847171	gaia.cs.umass.edu	192.168.1.109	TCP	108	[TCP Dup ACK 482#1] http(80) -> vnwk-prapi(2538) [ACK] Seq=1 Ack=436 Win=6432 Len=0
485	24.847267	Cisco-Li_f7:1d:51	Cisco-Li_f7:1d:51	802.11	38	Acknowledgement, Flags=.....C
486	24.848829	gaia.cs.umass.edu	192.168.1.109	TCP	415	http(80) -> vnwk-prapi(2538) [PSH, ACK] Seq=1 Ack=436 Win=6432 Len=313 [TCP segment of a reassembled
487	24.848950	Cisco-Li_f7:1d:51	Cisco-Li_f7:1d:51	802.11	38	Acknowledgement, Flags=.....C
488	24.850314	gaia.cs.umass.edu	192.168.1.109	TCP	1562	http(80) -> vnwk-prapi(2538) [ACK] Seq=314 Ack=436 Win=1460 [TCP segment of a reassembled PD
489	24.850809	gaia.cs.umass.edu	192.168.1.109	TCP	1562	[TCP Retransmission] http(80) -> vnwk-prapi(2538) [ACK] Seq=314 Ack=436 Win=6432 Len=1460

Frame 474 details: 110 bytes on wire (880 bits), 110 bytes captured (880 bits)

Frame 474: 110 bytes on wire (880 bits), 110 bytes captured (880 bits)

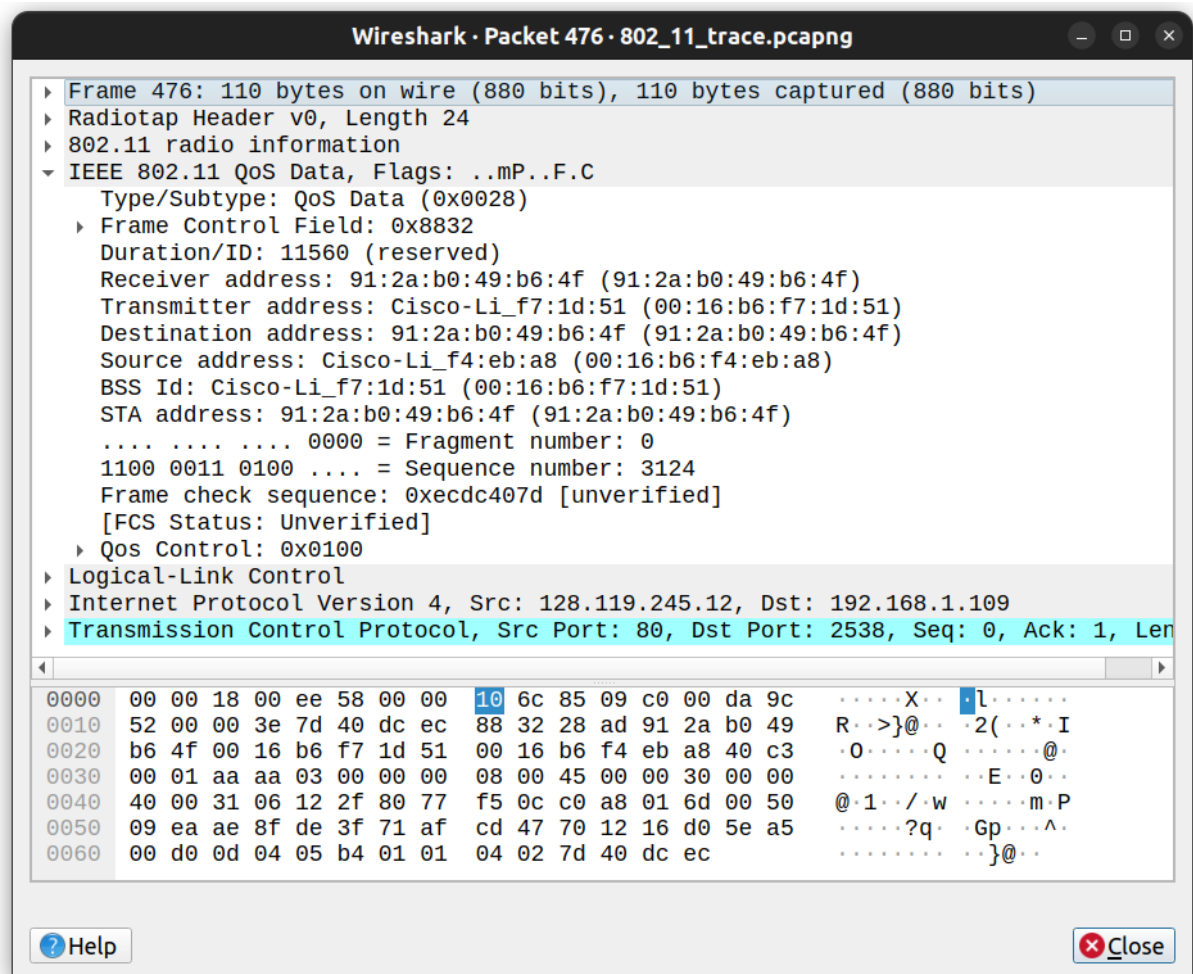
Summary: Packets: 2364 · Displayed: 2364 (100.0%) Profile: Default



7. Какие три поля MAC-адреса в стандарте 802.11? Какой MAC-адрес в этом кадре соответствует беспроводному хосту? Какой точке доступа? Какой маршрутизатору первого перехода? Каков IP-адрес беспроводного узла, отправляющего этот сегмент TCP? Какой IP-адрес назначения? Соответствует ли этот IP-адрес назначения хосту, точке доступа, маршрутизатору первого перехода или другому подключенному к сети устройству?

- MAC-адрес беспроводного хоста отправителя (Transmitter address, Source address) - 00:13:02:d1:b6:4f
- MAC-адрес точки доступа (Receiver address) - 00:16:b6:f7:1d:51
- MAC-адрес маршрутизатора первого перехода (Destination address) - 00:16:b6:f4:eb:a8
- IP-адрес отправителя - 192.168.1.109
- IP-адрес получателя (соответствует хосту gaia.cs.umass.edu) - 128.119.245.12

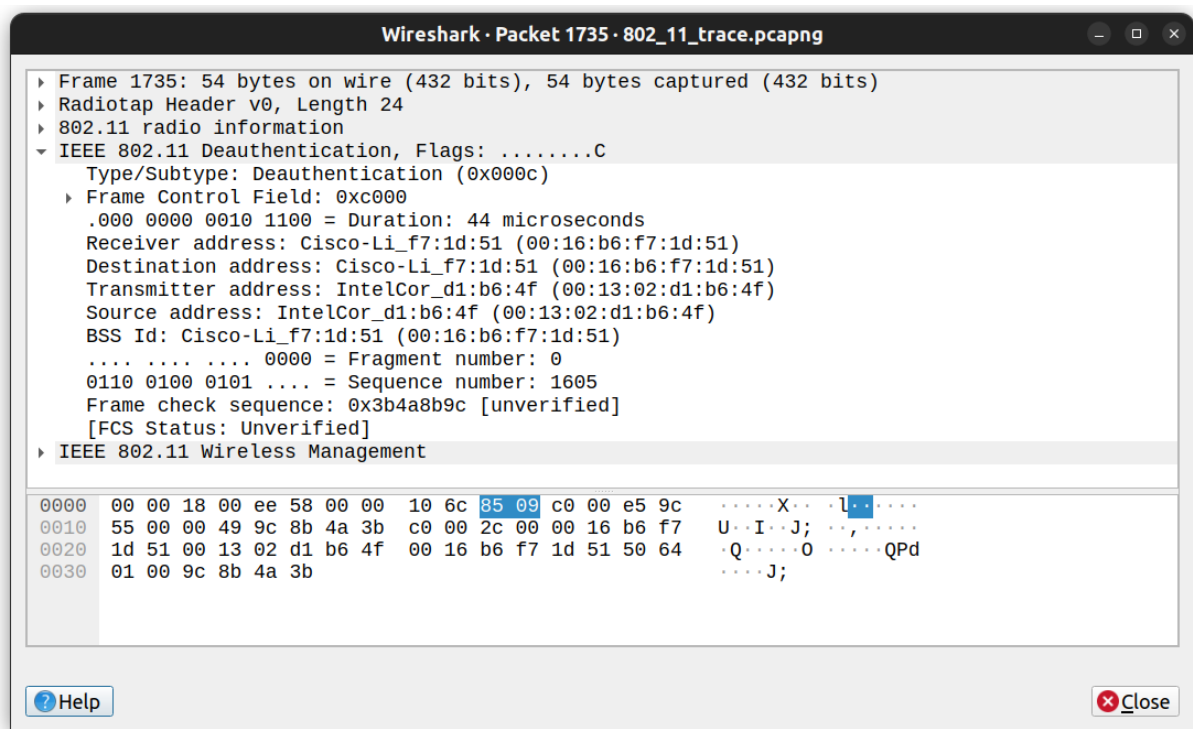
Найдите кадр 802.11, содержащий сегмент TCP SYN ACK для этого сеанса TCP.



8. Какие три поля MAC-адреса в кадре 802.11? Какой MAC-адрес в этом кадре соответствует хосту? Какой точке доступа? Какой маршрутизатору первого перехода? Соответствует ли MAC-адрес отправителя IP-адресу устройства, отправившего сегмент TCP, инкапсулированный в этой дейтаграмме?

- MAC-адрес хоста (Receiver address, Destination address) - 91:2a:b0:49:b6:4f
- MAC-адрес точки доступа (Transmitter address) - 00:16:b6:f7:1d:51
- MAC-адрес маршрутизатора первого перехода (Source address) - 00:16:b6:f4:eb:a8
- MAC-адрес отправителя (маршрутизатора первого перехода) не соответствует IP-адресу устройства, отправившего сегмент TCP (хоста gaia.cs.umass.edu)

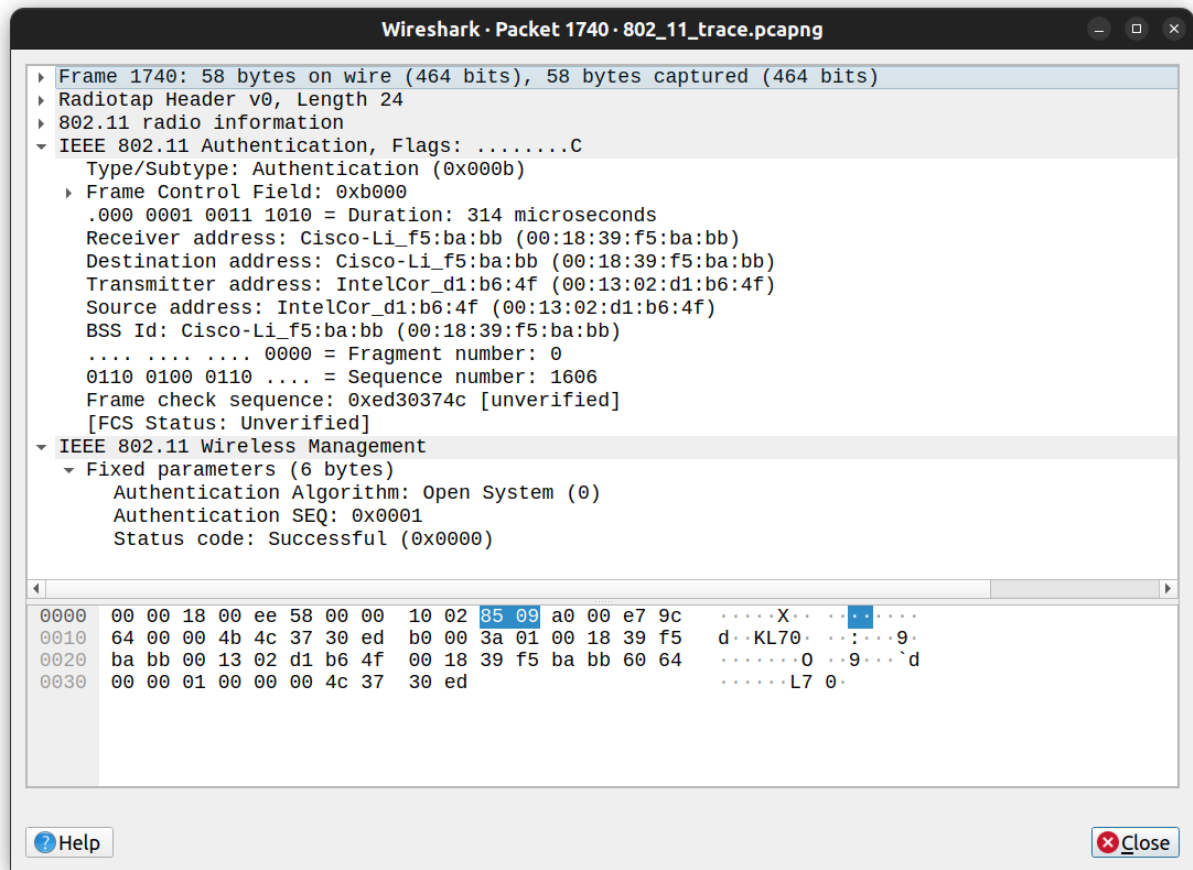
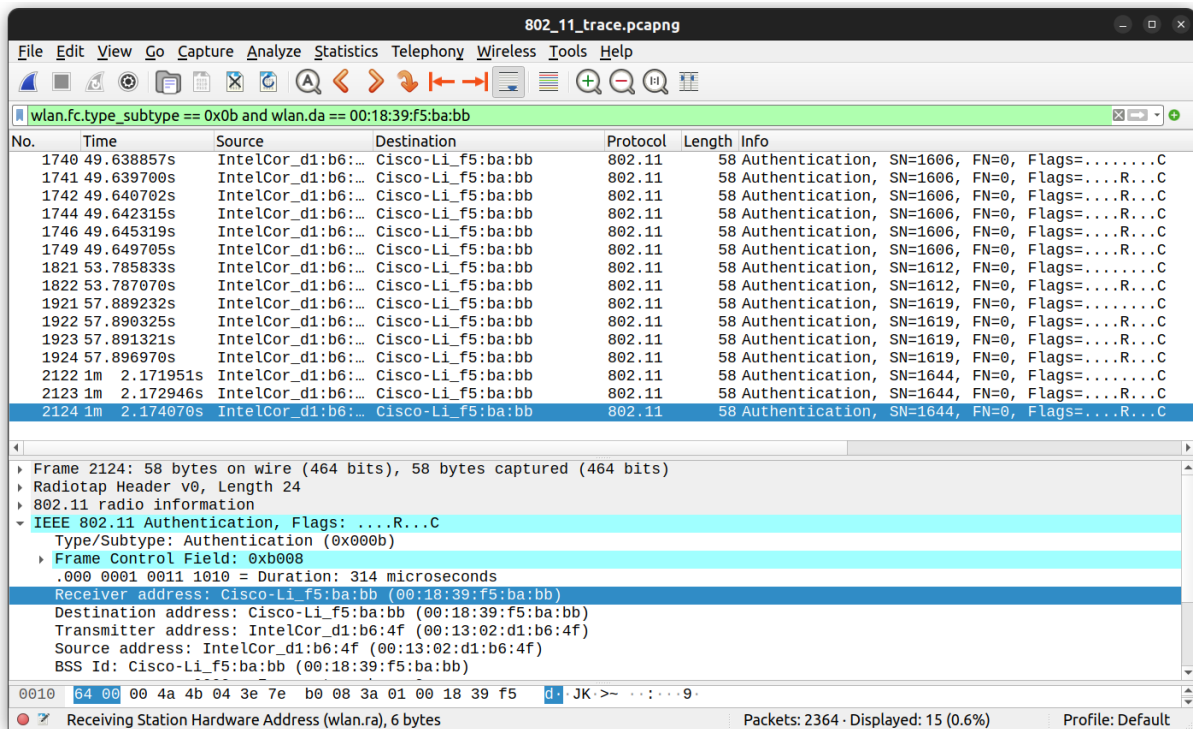
Ассоциация и диссоциация



9. Какие два действия предпринимаются хостом, чтобы завершить связь с точкой доступа 30 Монрое St, которая изначально была на месте, когда начался сбор трассировки? (Подсказка: одно из них - действие на уровне IP, а другое - действие на уровне 802.11). Глядя на спецификацию 802.11, есть ли еще один кадр, который вы, возможно, ожидали увидеть, но не видели здесь?

- Чтобы завершить связь с точкой доступа предпринимаются 2 действия: отключение от точки доступа (отправка Disassociation frame), отключение от текущей сети (отправка Deauthentication frame)
- Не обнаружен кадр Disassociation frame

Найдите кадры аутентификации, отправленные с хоста на точку доступа и наоборот.



10. Сколько сообщений AUTHENTICATION отправляется с беспроводного хоста на точку доступа *linksys_ses_24086* (с MAC-адресом Cisco_Li_f5:ba:bb)?

- Было отправлено 15 кадров

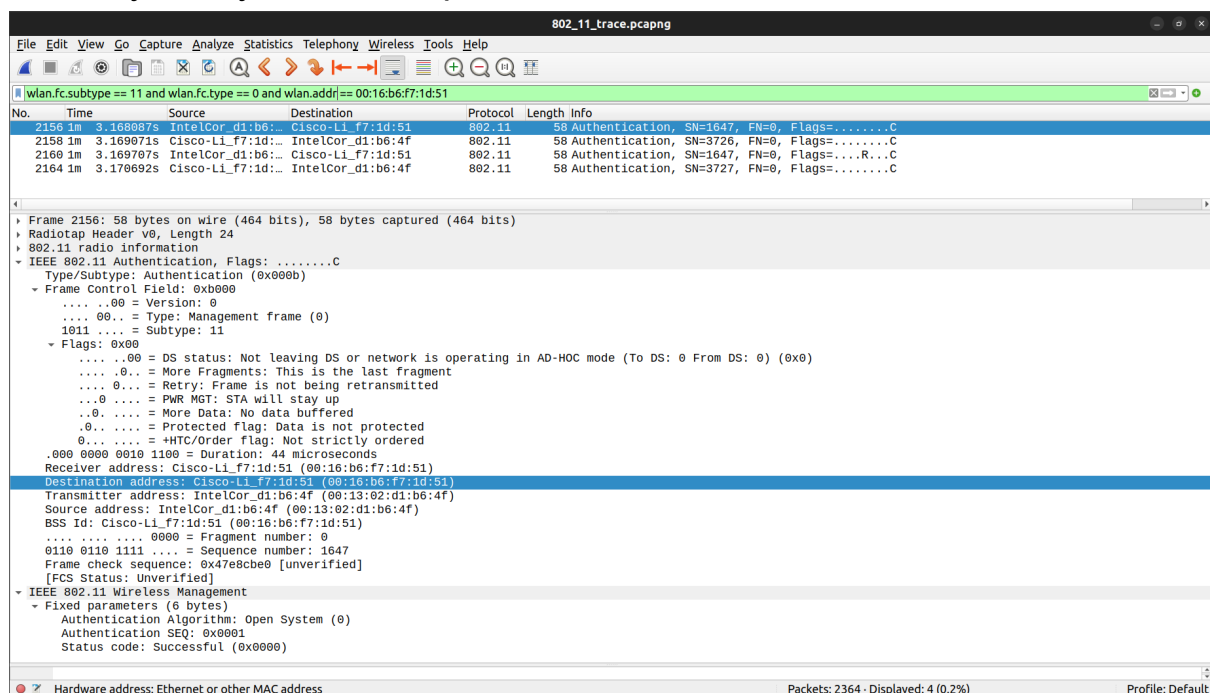
11. Хост хочет, чтобы аутентификация требовала ключа или была открытой?

- Значение поля Authentication Algorithm - 0 (Open System), т.е. аутентификация будет открытая

12. Видите ли вы в трассировке проверку подлинности ответа от точки доступа *linksys_ses_24086*?

- Проверки подлинности нет

Теперь давайте рассмотрим, что происходит, когда хост отказывается от попыток подключиться к точке доступа *linksys_ses_24086* и теперь пытается подключиться к точке доступа 30 Munroe St. Ищите кадры аутентификации, отправленные с хоста на точку доступа и наоборот.



13. В какое время поступает кадр AUTHENTICATION от хоста к точке доступа 30 Munroe St, и когда с этой точки доступа хосту в ответ отправляется ответный кадр AUTHENTICATION?

- В 1m 3.168087s поступает кадр AUTHENTICATION от хоста к точке доступа 30 Munroe St
- В 1m 3.169071s поступает ответный кадр

Рассмотрим ASSOCIATE REQUEST от хоста к точке доступа и соответствующий кадр ASSOCIATE RESPONSE от точки доступа к хосту.

802_11_trace.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Filter: wlan.fc.subtype < 2 and wlan.fc.type == 0 and wlan.addr == 00:16:b6:f7:1d:51

No.	Time	Source	Destination	Protocol	Length	Info
2162	1m 3.169918s	IntelCor_d1:b6:4f...	Cisco-Li_f7:1d:51	802.11	89	Association Request, SN=1648, FN=0, Flags=.....C, SSID=30 Munroe St
2166	1m 3.192101s	Cisco-Li_f7:1d:51...	IntelCor_d1:b6:4f	802.11	94	Association Response, SN=3728, FN=0, Flags=.....C

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
 - Type/Subtype: Association Request (0x0000)
 - Frame Control Field: 0x0000
 - 00 = Version: 0
 - 00 = Type: Management frame (0)
 - 0000 = Subtype: 0
 - Flags: 0x00
 - 00 = DS status: Not leaving DS or network is operating in AD-HOC mode (To DS: 0 From DS: 0) (0x0)
 - 00 = More Fragments: This is the last fragment
 - 00 = 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 = HTT/Order Flag: Not strictly ordered
 - .000 0000 0010 1100 = Duration: 44 microseconds
 - Receiver address: Cisco-Li_f7:1d:51 (00:16:b6:f7:1d:51)
 - Destination address: Cisco-Li_f7:1d:51 (00:16:b6:f7:1d:51)
 - Transmitter address: IntelCor_d1:b6:4f (00:13:02:d1:b6:4f)
 - 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)
 - 0000 = Fragment number: 0
 - 0110 0111 0000 = Sequence number: 1648
 - Frame check sequence: 0xfe3badc6 [unverified]
 - [FCS Status: Unverified]
 - IEEE 802.11 Wireless Management
 - Fixed parameters (4 bytes)
 - Capabilities Information: 0xce01
 - Listen Interval: 0x000a
 - Tagged parameters (33 bytes)
 - Tag: SSID parameter set: 30 Munroe St

Destination Hardware Address (wlan.da), 6 bytes

Packets: 2364 · Displayed: 2 (0.1%)

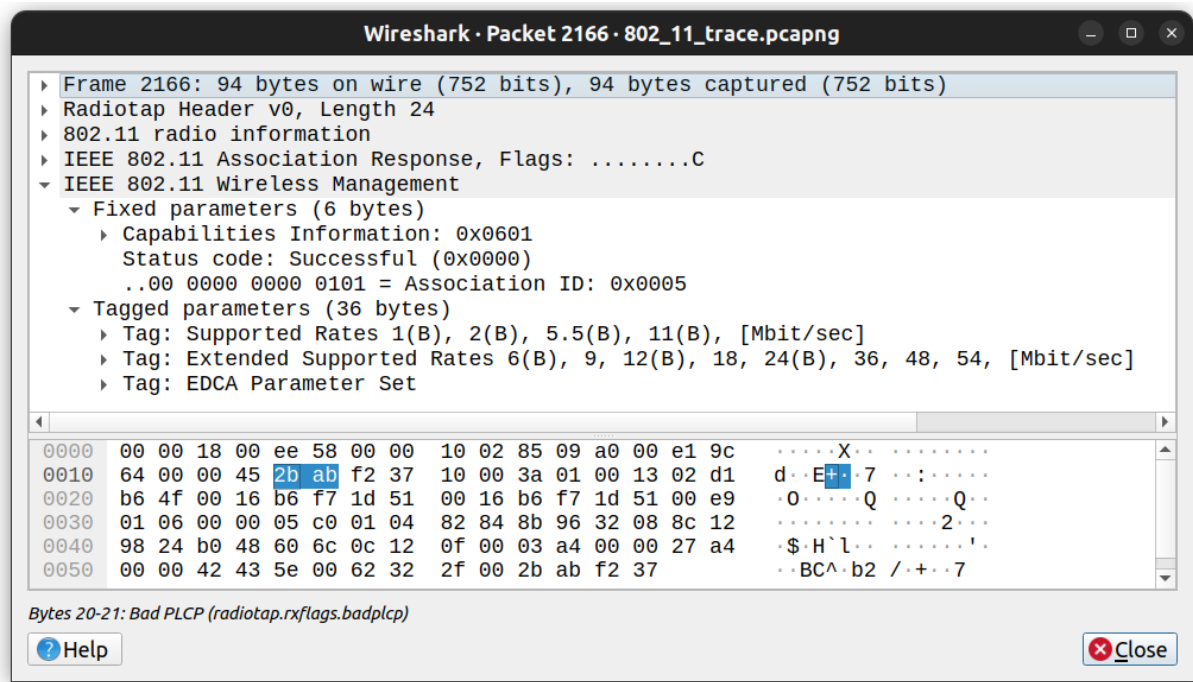
Profile: Default

Wireshark · Packet 2162 · 802_11_trace.pcapng

- 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)
 - Capabilities Information: 0xce01
 - Listen Interval: 0x000a
 - 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]

0000	00 00 18 00 ee 58 00 00	10 6c 85 09 c0 00 e3 9cX...l.....
0010	64 00 00 47 c6 ad 3b fe	00 00 2c 00 00 16 b6 f7	d..G...;.....
0020	1d 51 00 13 02 d1 b6 4f	00 16 b6 f7 1d 51 00 67	.Q.....0.....Q.g
0030	01 ce 0a 00 00 0c 33 30	20 4d 75 6e 72 6f 65 2030 Munroe
0040	53 74 01 08 82 84 8b 96	8c 12 98 24 2e 01 00 32	St.....\$....2
0050	04 b0 48 60 6c c6 ad 3b	fe	..H`l...;

Help Close



14. В какое время появился ASSOCIATE REQUEST от хоста к точке доступа 30 Munroe St? Когда отправляется соответствующий ответ ASSOCIATE RESPONSE?

- В 1m 3.169910s поступает кадр ASSOCIATE REQUEST от хоста к точке доступа 30 Munroe St
- В 1m 3.192101s поступает ответный кадр ASSOCIATE RESPONSE

15. Какие скорости передачи использует хост? Какие точка доступа?

- Хост использует следующие скорости передачи: 1, 2, 5.5, 11, 6, 9, 12, 18 Мбит/с
- Точка доступа использует следующие скорости передачи: 1, 2, 5.5, 11 Мбит/с

Другие типы кадров

802_11_trace.pcapng					
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help					
[wlan.fc.subtype == 4 or wlan.fc.subtype == 5] and wlan.fc.type == 0					
No.	Time	Source	Destination	Protocol	Length Info
50	2.297613s	IntelCor_1f:57:13	Broadcast	802.11	79 Probe Request, SN=576, FN=0, Flags=.....C, SSID=Home WIFI
51	2.300697s	Cisco-Li_f7:1d:13	IntelCor_1f:57:13	802.11	177 Probe Response, SN=2878, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
52	2.302191s	Cisco-Li_f7:1d:13	IntelCor_1f:57:13	802.11	177 Probe Response, SN=2878, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
53	2.304063s	Cisco-Li_f7:1d:13	IntelCor_1f:57:13	802.11	177 Probe Response, SN=2878, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
54	2.305562s	Cisco-Li_f7:1d:13	IntelCor_1f:57:13	802.11	177 Probe Response, SN=2878, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
55	2.308558s	Cisco-Li_f7:1d:13	IntelCor_1f:57:13	802.11	177 Probe Response, SN=2878, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
56	2.310072s	Cisco-Li_f7:1d:13	IntelCor_1f:57:13	802.11	177 Probe Response, SN=2878, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
59	2.453941s	Cisco-Li_f7:1d:13	IntelCor_1f:57:13	802.11	177 Probe Response, SN=2881, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
83	4.283835s	Cisco-Li_f7:1d:13	IntelCor_d1:b6:4f	802.11	177 Probe Response, SN=2900, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
87	4.298449s	IntelCor_1f:57:13	Broadcast	802.11	78 Probe Request, SN=598, FN=0, Flags=.....C, SSID=phoiphass
88	4.301564s	Cisco-Li_f7:1d:13	IntelCor_1f:57:13	802.11	177 Probe Response, SN=2901, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
89	4.303314s	Cisco-Li_f7:1d:13	IntelCor_1f:57:13	802.11	177 Probe Response, SN=2901, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
90	4.304814s	Cisco-Li_f7:1d:13	IntelCor_1f:57:13	802.11	177 Probe Response, SN=2901, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
93	4.403454s	Cisco-Li_f7:1d:13	IntelCor_1f:57:13	802.11	177 Probe Response, SN=2903, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
94	4.404939s	Cisco-Li_f7:1d:13	IntelCor_1f:57:13	802.11	177 Probe Response, SN=2903, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
117	6.299705s	IntelCor_1f:57:13	Broadcast	802.11	79 Probe Request, SN=620, FN=0, Flags=.....C, SSID=concourse
118	6.300439s	IntelCor_1f:57:13	Broadcast	802.11	70 Probe Request, SN=621, FN=0, Flags=.....C, SSID=Wildcard (Broadcast)
119	6.303313s	Cisco-Li_f7:1d:13	IntelCor_1f:57:13	802.11	177 Probe Response, SN=2922, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
130	6.404446s	Cisco-Li_f7:1d:13	IntelCor_1f:57:13	802.11	177 Probe Response, SN=2924, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
131	6.405938s	Cisco-Li_f7:1d:13	IntelCor_1f:57:13	802.11	177 Probe Response, SN=2924, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
132	6.407522s	Cisco-Li_f7:1d:13	IntelCor_1f:57:13	802.11	177 Probe Response, SN=2924, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
133	6.409063s	Cisco-Li_f7:1d:13	IntelCor_1f:57:13	802.11	177 Probe Response, SN=2924, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
134	6.410562s	Cisco-Li_f7:1d:13	IntelCor_1f:57:13	802.11	177 Probe Response, SN=2924, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
135	6.412063s	Cisco-Li_f7:1d:13	IntelCor_1f:57:13	802.11	177 Probe Response, SN=2924, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
136	6.413562s	Cisco-Li_f7:1d:13	IntelCor_1f:57:13	802.11	177 Probe Response, SN=2924, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
138	6.455573s	Cisco-Li_f7:1d:13	IntelCor_1f:57:13	802.11	177 Probe Response, SN=2926, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
139	6.457064s	Cisco-Li_f7:1d:13	IntelCor_1f:57:13	802.11	177 Probe Response, SN=2926, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
140	6.458567s	Cisco-Li_f7:1d:13	IntelCor_1f:57:13	802.11	177 Probe Response, SN=2926, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
141	6.460063s	Cisco-Li_f7:1d:13	IntelCor_1f:57:13	802.11	177 Probe Response, SN=2926, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
142	6.461563s	Cisco-Li_f7:1d:13	IntelCor_1f:57:13	802.11	177 Probe Response, SN=2926, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
143	6.463062s	Cisco-Li_f7:1d:13	IntelCor_1f:57:13	802.11	177 Probe Response, SN=2926, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
144	6.464563s	Cisco-Li_f7:1d:13	IntelCor_1f:57:13	802.11	177 Probe Response, SN=2926, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
156	7.355808s	Cisco-Li_f7:1d:13	IntelCor_d1:b6:4f	802.11	177 Probe Response, SN=2936, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
171	8.299988s	IntelCor_1f:57:13	Broadcast	802.11	77 Probe Request, SN=642, FN=0, Flags=.....C, SSID=linksys
173	8.303507s	Cisco-Li_f7:1d:13	IntelCor_1f:57:13	802.11	177 Probe Response, SN=2946, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
174	8.305056s	Cisco-Li_f7:1d:13	IntelCor_1f:57:13	802.11	177 Probe Response, SN=2946, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
175	8.306687s	Cisco-Li_f7:1d:13	IntelCor_1f:57:13	802.11	177 Probe Response, SN=2946, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St

Wireshark · Packet 50 · 802_11_trace.pcapng

▶ 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

.0000 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

▼ Tagged parameters (27 bytes)

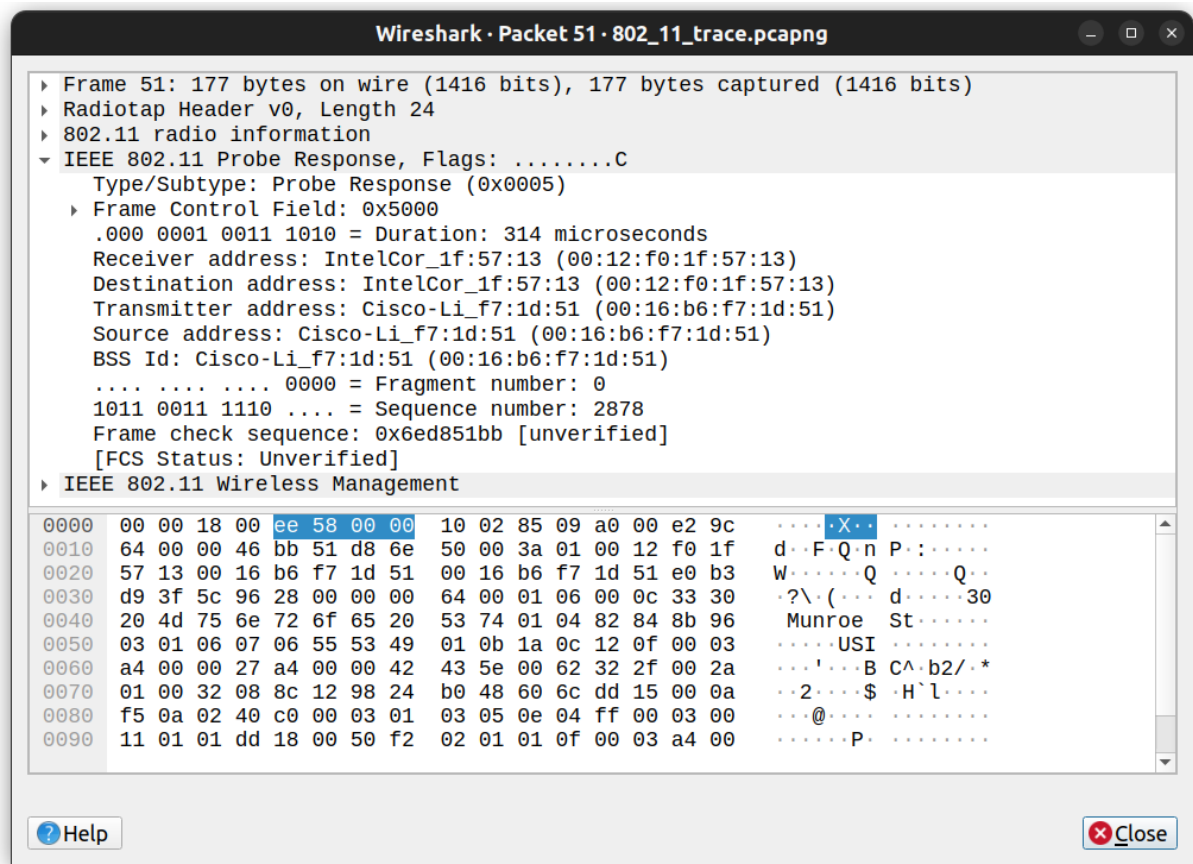
▶ Tag: SSID parameter set: Home WIFI

▶ Tag: Supported Rates 1(B), 2(B), 5.5, 11, 6, 9, 12, 18, [Mbit/sec]

▶ Tag: Extended Supported Rates 24, 36, 48, 54, [Mbit/sec]

Help

Close



16. Каковы MAC-адреса отправителя, получателя и BSS ID в этих кадрах? Какова цель этих двух типов кадров?

- MAC-адрес отправителя в кадре Probe Request - 00:12:f0:1f:57:13 (Хост)
- MAC-адрес получателя в кадре Probe Request - ff:ff:ff:ff:ff:ff (Broadcast)
- BSS ID в кадре Probe Request - ff:ff:ff:ff:ff:ff (Broadcast)
- MAC-адрес отправителя в кадре Probe Response - 00:16:b6:f7:1d:51 (Точка доступа)
- MAC-адрес получателя в кадре Probe Response - 00:12:f0:1f:57:13 (Хост)
- BSS ID в кадре Probe Response - 00:16:b6:f7:1d:51 (Точка доступа)
- Данные кадры используются для активного сканирования