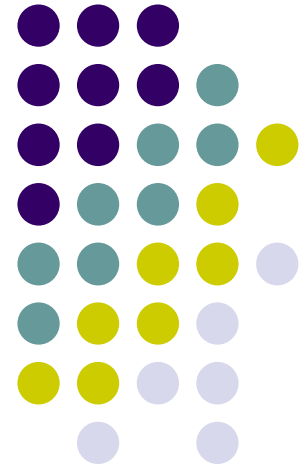


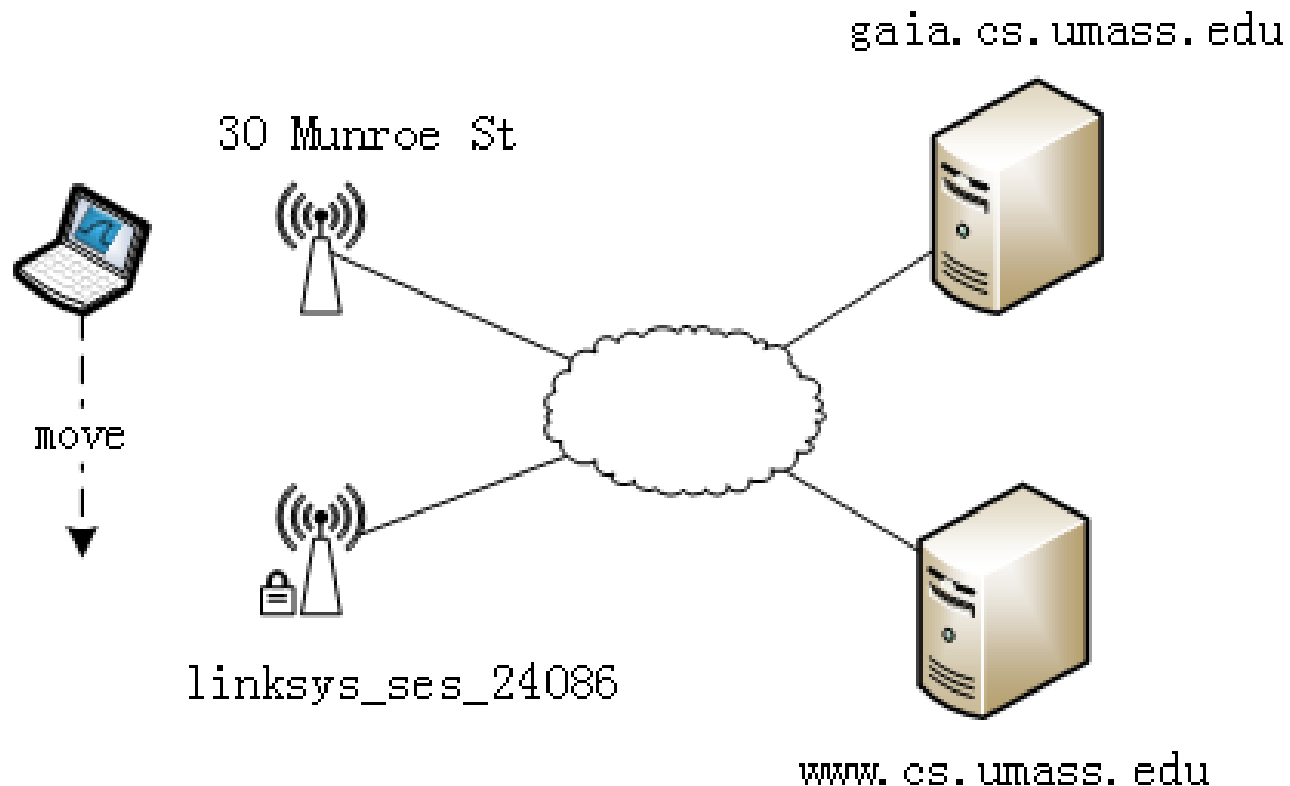
802.11 Trace Analysis



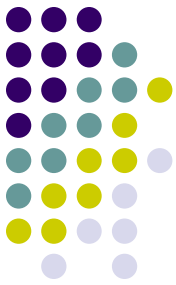


Packet Trace

- Download “Wireshark_802_11.pcap” from bb.ustc.edu.cn



Packet Trace



● Open “Wireshark 802_11.pcap” with Wireshark

Wireshark 802_11.pcap

文件(F) 编辑(E) 视图(V) 跳转(G) 捕获(C) 分析(A) 统计(S) 电话(V) 无线(W) 工具(T) 帮助(H)

应用显示过滤器: <Ctrl-/->

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=2854, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
2	0.062101	b6:78:8c:c1:ae:c0 (...)	65:a8:d5:b2:c1:99 (...)	802.11	1624	802.11 Block Ack Req, Flags=op.P...TC
3	0.085474	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=2855, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
4	0.187919	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=2856, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
5	0.188100	IntelCor_d1:b6:4f	Cisco-Li_f7:1d:51	802.11	54	QoS Null function (No data), SN=1482, FN=0, Flags=.....TC
6	0.188201		IntelCor_d1:b6:4f (...)	802.11	38	Acknowledgement, Flags=.....C
7	0.188935	IntelCor_d1:b6:4f	Cisco-Li_f7:1d:51	802.11	54	QoS Null function (No data), SN=1483, FN=0, Flags=...P...TC
8	0.189034		IntelCor_d1:b6:4f (...)	802.11	38	Acknowledgement, Flags=.....C
9	0.290284	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=2857, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
10	0.294432	LinksysG_67:22:94	Broadcast	802.11	90	Beacon frame, SN=3072, FN=0, Flags=.....C, BI=62, SSID=li001\0040[Malformed Packet]
11	0.393174	Cisco-Li_f7:1d:51	Broadcast	802.11	183	Beacon frame, SN=2858, FN=0, Flags=.....C, BI=100, SSID=30 Munroe St
12	0.396690	00:ae:93:3d:0a:4a	ff:ff:ff:ff:bf:4a	802.11	90	Association Response, SN=3073, FN=0, Flags=.....C
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
14	0.499197	LinksysG_67:22:94	Broadcast	802.11	90	Beacon frame, SN=3074, FN=0, Flags=.....C, BI=100, SSID=linksys12

> 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 0111 = Sequence number: 2855

Frame check sequence: 0x39700f3d [unverified]

[FCS Status: Unverified]

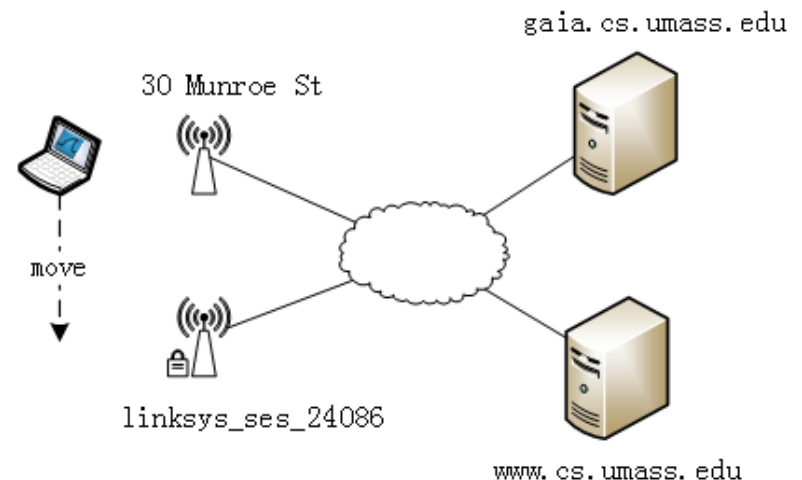
> IEEE 802.11 Wireless Management

```
0000 00 00 18 00 ee 58 00 00 10 02 85 09 a0 00 e2 9c .....X.....
0010 52 00 00 46 3d 0f 70 39 80 00 00 00 ff ff ff ff R..F=p9.....
0020 ff ff 00 16 b6 f7 1d 51 00 16 b6 f7 1d 51 70 b2 .....Q.....Qp
0030 82 71 3a 96 28 00 00 00 64 00 01 06 00 0c 33 30 .q:.(...d...30
0040 20 4d 75 6e 72 6f 65 20 53 74 01 04 82 84 8b 96 Munroe St.....
0050 03 01 06 05 04 00 01 00 00 07 06 55 53 49 01 0b .....USI..
0060 1a 0c 12 0f 00 03 a4 00 00 27 a4 00 00 42 43 5e .....BC^
0070 00 62 32 2f 00 2a 01 00 32 08 8c 12 98 24 b0 48 .b2/*..2....$-H
0080 60 6c dd 15 00 0a f5 0a 02 40 c0 00 03 01 03 05 ^l.....@.....
0090 0e 04 ff 00 03 00 11 01 01 dd 18 00 50 f2 02 01 .....P.....
00a0 01 0f 00 03 a4 00 00 27 a4 00 00 42 43 5e 00 62 .....BC^b
00b0 32 2f 00 3d 0f 70 39 2/-=p9
```



Packet Trace

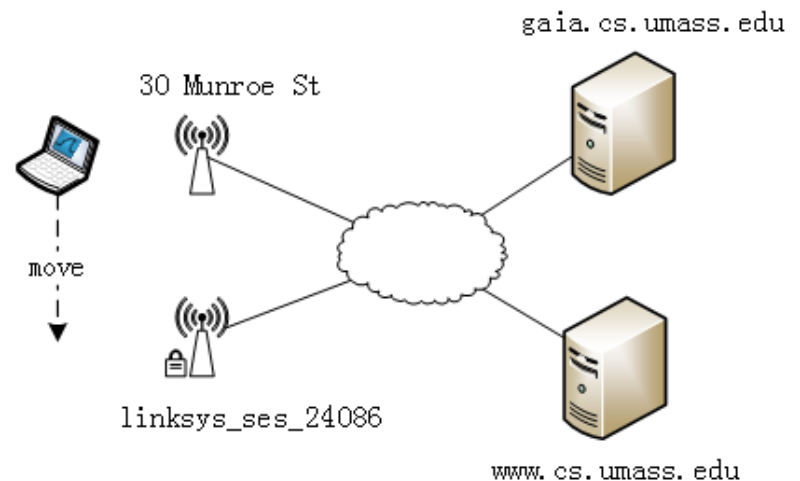
- How this trace is captured?
 - The host is already associated with the 30 Munroe St AP when the trace begins.
 - At $t = 24.82$, the host makes an HTTP request to <http://gaia.cs.umass.edu/wireshark-labs/alice.txt>. The IP address of gaia.cs.umass.edu is 128.119.245.12.





Packet Trace

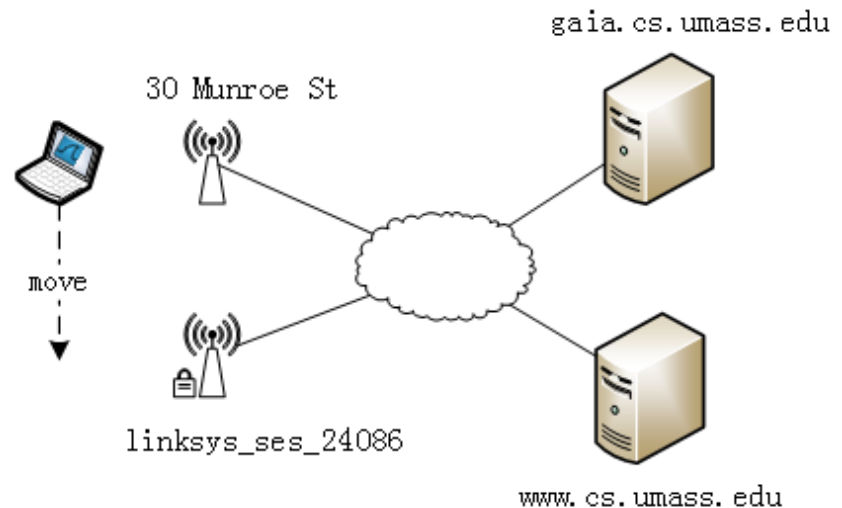
- At $t=32.82$, the host makes an HTTP request to <http://www.cs.umass.edu>, whose IP address is 128.119.240.19.
- At $t = 49.58$, the host disconnects from the 30 Munroe St AP and attempts to connect to the linksys_ses_24086. This is not an open access point, and so the host is eventually unable to connect to this AP.





Packet Trace

- At $t=63.0$ the host gives up trying to associate with the linksys_ses_24086 AP, and associates again with the 30 Munroe St access point.





Questions

1. What are the SSIDs of the two APs that are issuing most of the beacon frames in this trace? [10%]
2. What are the three addresses in the Beacon frame from the two APs respectively. [15%]

2	2	6	6	6	2	6	0 - 2312	4
frame control	duration	address 1	address 2	address 3	seq control	address 4	payload	CRC



Questions

3. How many APs the wireless laptop has received Beacon frames from? List their MAC addresses. Why the laptop can receive frames from an AP even though it does not associate with the AP? [15%]
4. Find the 802.11 frame containing the SYN TCP segment for this first TCP session (that downloads alice.txt). What are the three MAC addresses in the frame, which is the address for wireless laptop / AP / first-hop router? [15%]

Questions



5. For the SYN-ACK segment of the first TCP session, what are the three MAC addresses in the frame, and which is the address for wireless laptop / AP / first-hop router? [15%]
6. For the above mentioned SYN-ACK segment, is the sender MAC address corresponds to the web server's IP address? Why? [10%]



Questions

7. What two actions are taken (i.e., frames are sent) by the host in the trace just after $t=49$, to end the association with the *30 Munroe St* AP? [10%]
8. Can you capture a similar trace? Why or why not? [10%]



Submission

- Submit to bb.ustc.edu.cn
 1. A pdf file named “id + name + Trace_analysis.pdf”
 2. For Q1 – Q5, you need to give the answer and give a screenshot of the information of the beacon frame in Wireshark.
 3. For Q6 – Q8, you need to give your answer and a brief explanation.
 4. Deadline: **2022/01/25**