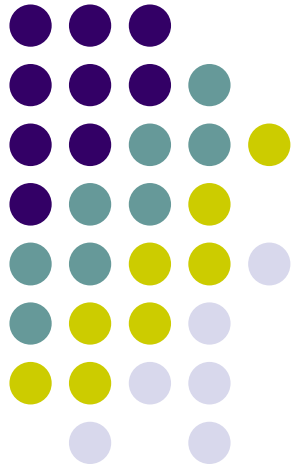
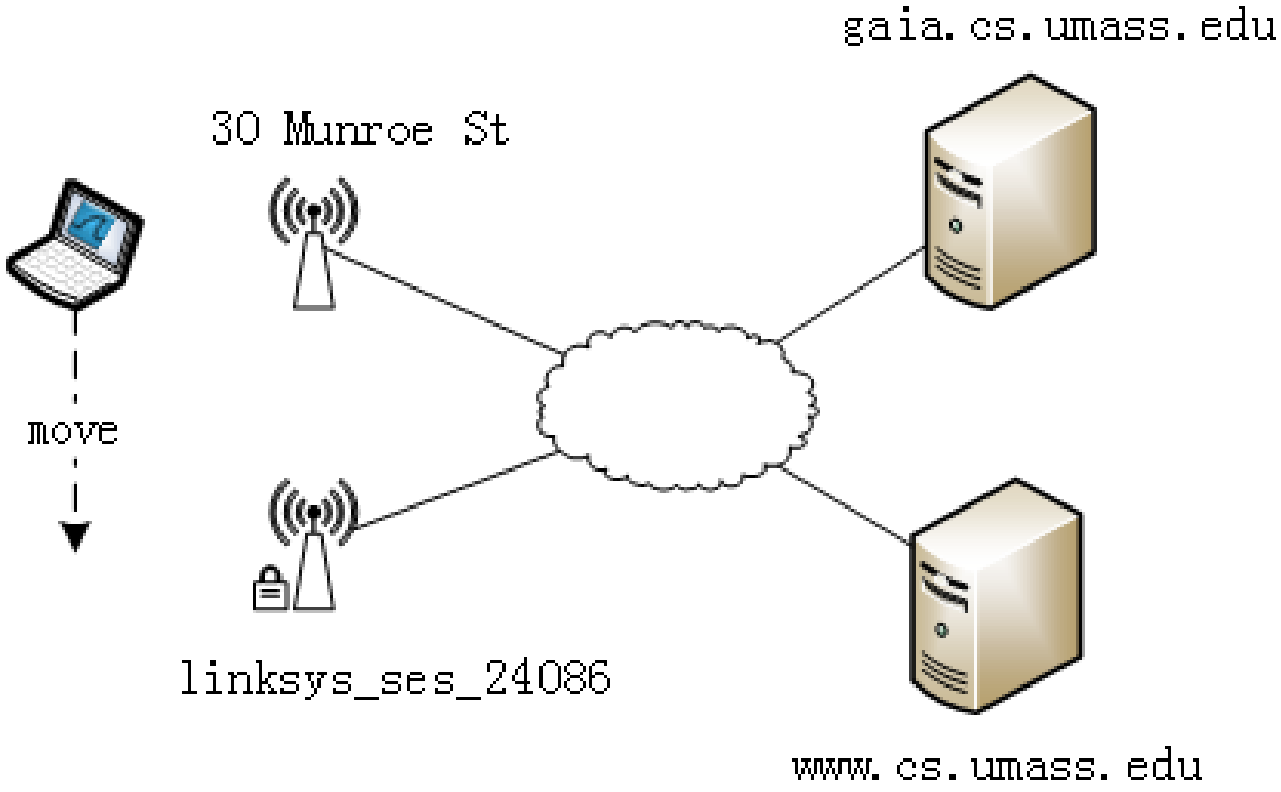
802.11 Trace Analysis



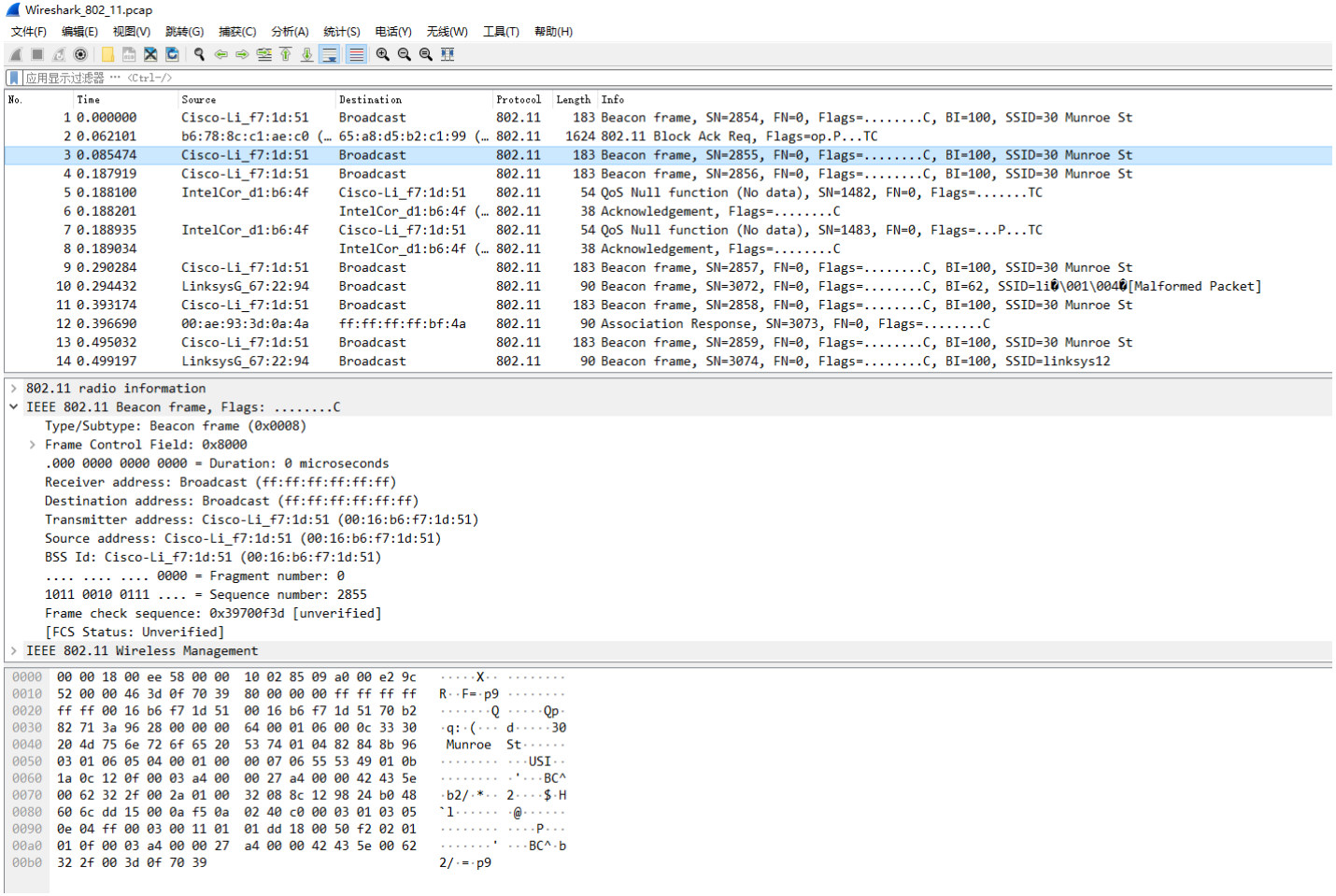
Packet Trace

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



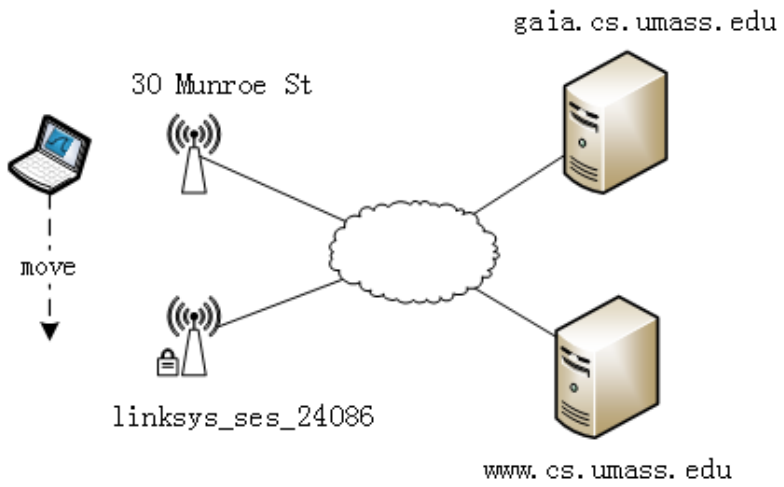
Packet Trace

- Open “Wireshark_802_11.pcap” with Wireshark



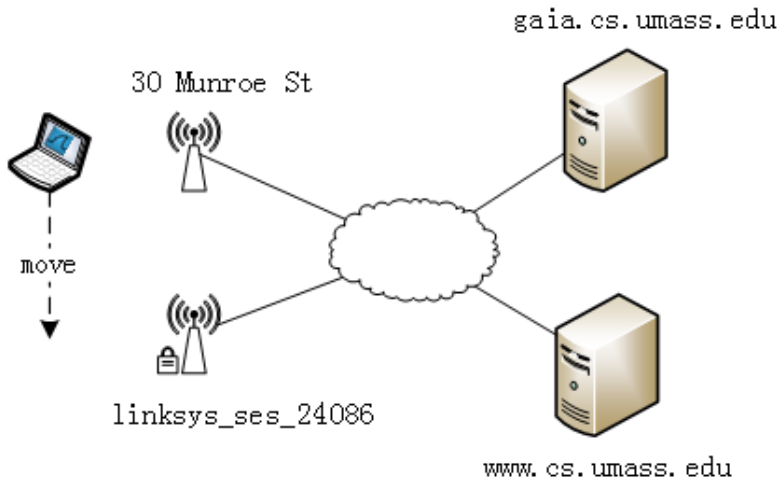
Packet Trace

- 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.



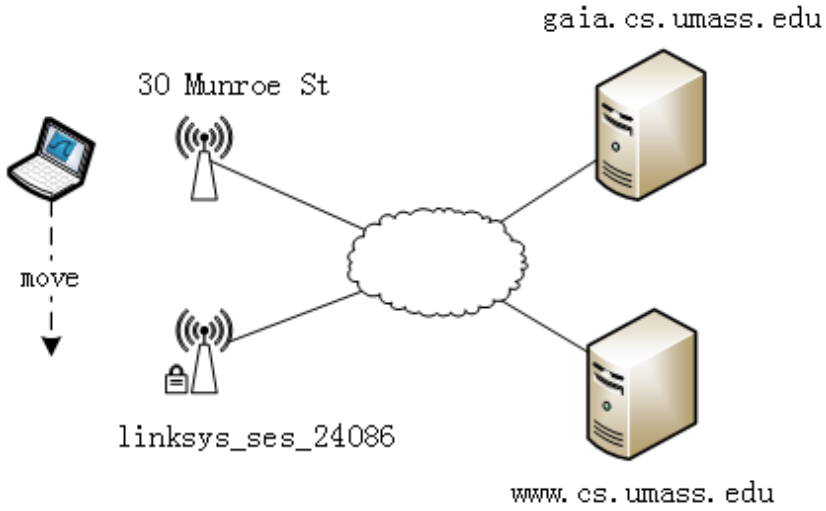
Packet Trace

- 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.



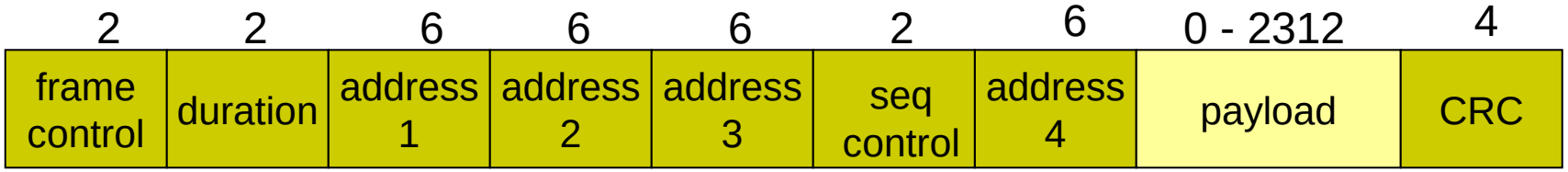
Packet Trace

- 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%]



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