Wireshark Analysis and Riverbed Modeling of WLANs

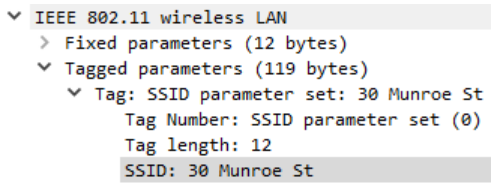
Kangyan XU

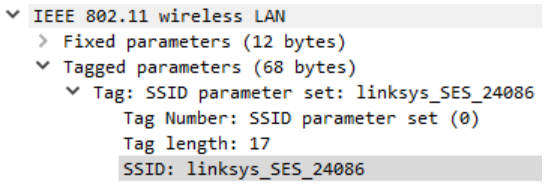
Brief Abstract

This report has two parts.
The first part uses Wireshark to analyze frames transferred between AP and stations, which helps to have a better understanding on how Wi-Fi works.
The second part uses Riverbed to model WLAN, focuses on how to improve the network performance.

Wireshark Analysis Questions

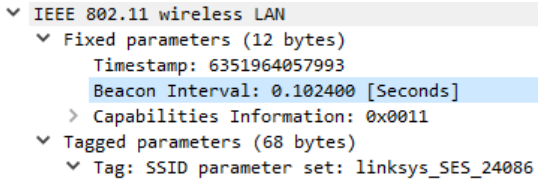
1. What are the SSIDs of the two access points that are issuing most of the beacon frames in this trace?

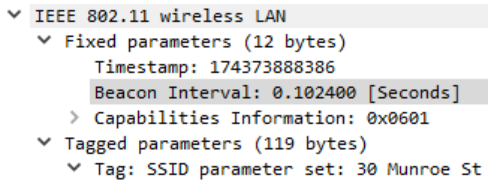




A: SSID: 30 Munroe St
SSID: linksys_SES_24086

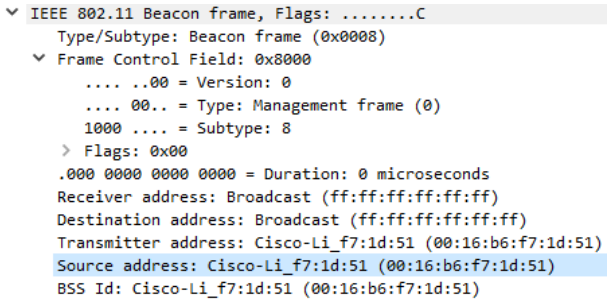
2. What are the intervals of time between the transmissions of the beacon frames the linksys_ses_24086 access point? From the 30 Munroe St. access point? (Hint: this interval of time is contained in the beacon frame itself).

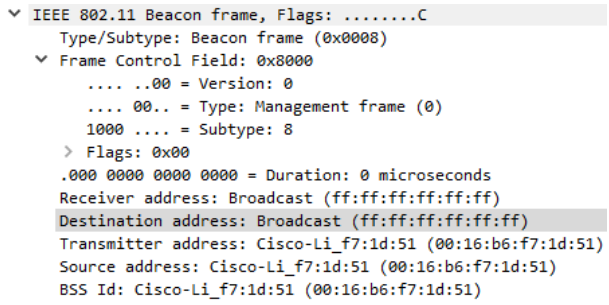




A: Both APs' Beacon Interval Time are the same 0.1024 seconds.

3. What (in hexadecimal notation) is the source MAC address on the beacon frame from 30 Munroe St? Recall from Figure 7.13 in the text that the source, destination, and BSS are three addresses used in an 802.11 frame.





A: The source MAC address is 00:16:b6:f7:1d:51

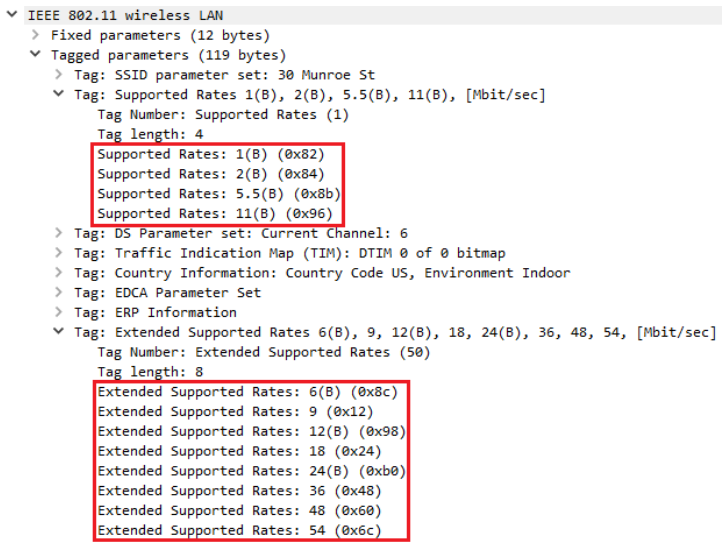
4. What (in hexadecimal notation) is the destination MAC address on the beacon frame from 30 Munroe St?

A: The destination MAC address is ff:ff:ff:ff:ff:ff (broadcast).

5. What (in hexadecimal notation) is the MAC BSS id on the beacon frame from 30 Munroe St?

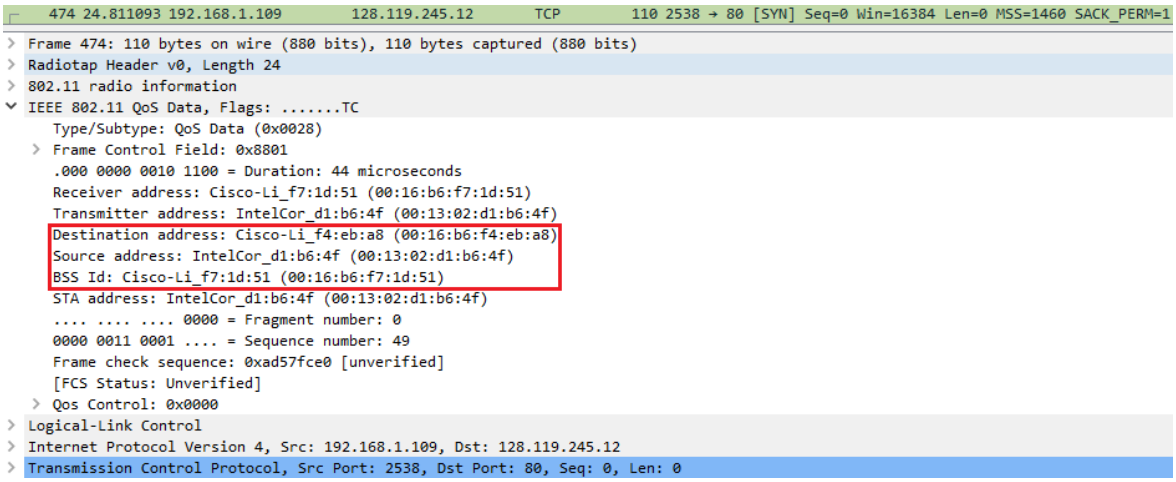
A: The MAC BSS id is also 00:16:b6:f7:1d:51

6. The beacon frames from the 30 Munroe St access point advertise that the access point can support four data rates and eight additional "extended supported rates." What are these rates?

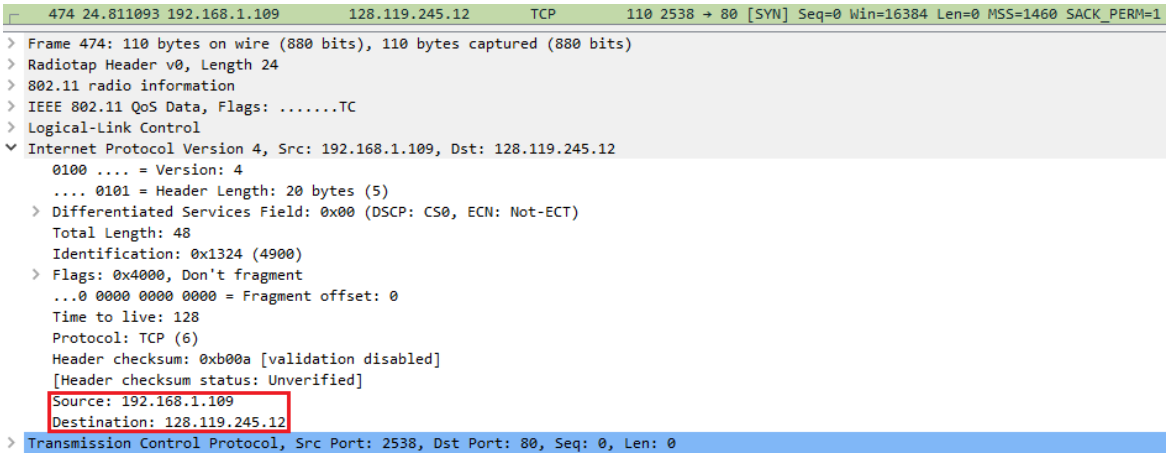


A: Four data rates are 1, 2, 5.5, 11 (Mbps). Eight additional rates are 6, 9, 12, 18, 24, 36, 48, 54 (Mbps).

7. Find the 802.11 frame containing the SYN TCP segment for this first TCP session (that downloads alice.txt). What are three MAC address fields in the 802.11 frame? Which MAC address in this frame corresponds to the wireless host (give the hexadecimal representation of the MAC address for the host)? To the access point? To the first-hop router? What is the IP address of the wireless host sending this TCP segment? What is the destination IP address? Does this destination IP address correspond to the host, access point, first-hop router, or some other network-attached device? Explain.

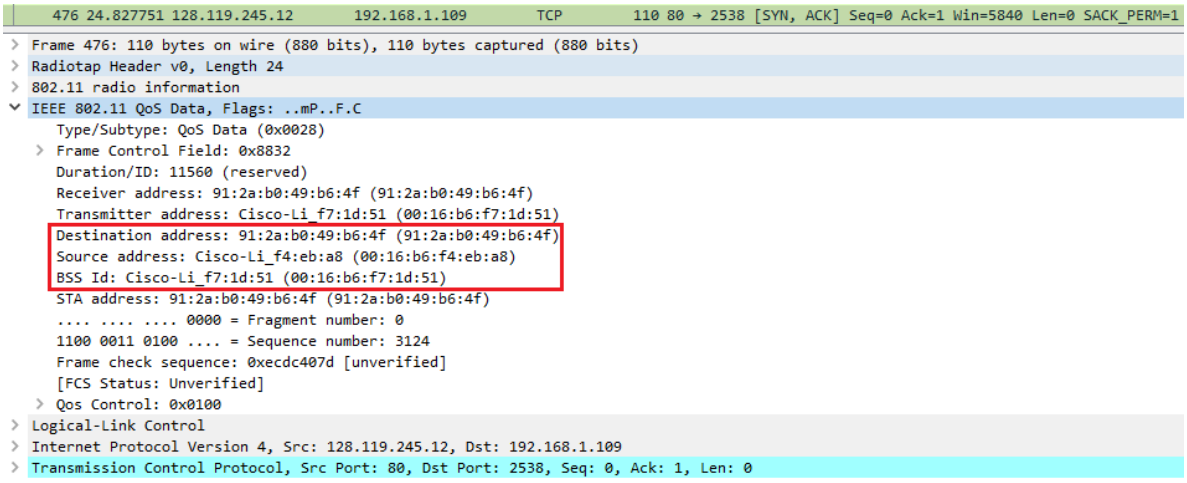


A: MAC address: wireless host (00:13:02:d1:b6:4f), AP (00:16:b6:f7:1d:51), first-hop router (00:16:b6:f4:eb:a8).

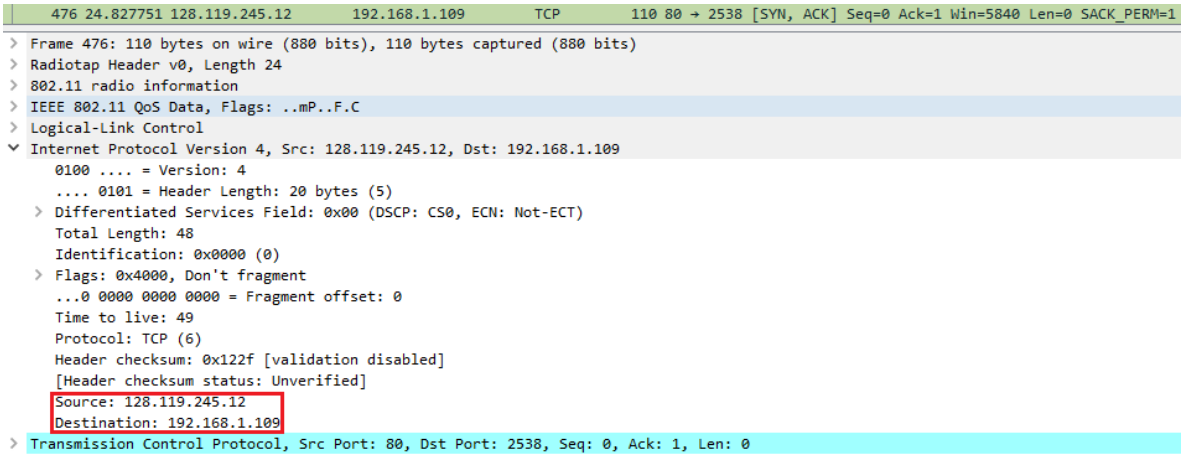


A: IP address of wireless host: 192.168.1.109, destination IP address: 128.119.245.12
This destination IP address correspond to the server of “gaia.cs.umass.edu”.

8. Find the 802.11 frame containing the SYNACK segment for this TCP session. What are three MAC address fields in the 802.11 frame? Which MAC address in this frame corresponds to the host? To the access point? To the first-hop router? Does the sender MAC address in the frame correspond to the IP address of the device that sent the TCP segment encapsulated within this datagram?



A: MAC address: wireless host (91:2a:b0:49:b6:4f), AP (00:16:b6:f7:1d:51), first-hop router (00:16:b6:f4:eb:a8).



A: The sender MAC (first-hop router) not correspond to the IP (server of “gaia.cs.umass.edu”).

9. 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 that was initially in place when trace collection began? (Hint: one is an IP-layer action, and one is an 802.11-layer action). Looking at the 802.11 specification, is there another frame that you might have expected to see, but don't see here?

1733	49.583615	192.168.1.109	192.168.1.1	DHCP	390 DHCP Release - Transaction ID 0xea5a526
1734	49.583771		IntelCor_d1:b6:4f (…	802.11	38 Acknowledgement, Flags=........C
1735	49.609617	IntelCor_d1:b6:4f	Cisco-Li_f7:1d:51	802.11	54 Deauthentication, SN=1605, FN=0, Flags=........C
1736	49.609770		IntelCor_d1:b6:4f (…	802.11	38 Acknowledgement, Flags=........C
1737	49.614478	IntelCor_d1:b6:4f	Broadcast	802.11	99 Probe Request, SN=1606, FN=0, Flags=........C, SSID=linksys_SES_24086
1738	49.615869		Cisco-Li_f5:ba:bb (…	802.11	38 Acknowledgement, Flags=........C
1739	49.617713		Cisco-Li_f5:ba:bb (…	802.11	38 Acknowledgement, Flags=........C
1740	49.638857	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58 Authentication, SN=1606, FN=0, Flags=........C
1741	49.639700	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58 Authentication, SN=1606, FN=0, Flags=....R...C
1742	49.640702	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58 Authentication, SN=1606, FN=0, Flags=....R...C
1743	49.641910		Cisco-Li_f5:ba:bb (…	802.11	38 Acknowledgement, Flags=........C
1744	49.642315	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58 Authentication, SN=1606, FN=0, Flags=....R...C

A: DHCP Release and Deauthentication. Not sure which another frame is expected to see.

10. Examine the trace file and look for AUTHENICATION frames sent from the host to an AP and vice versa. How many AUTHENTICATION messages are sent from the wireless host to the linksys_ses_24086 AP (which has a MAC address of Cisco_Li_f5:ba:bb) starting at around t=49?

A: The list of A**UTHENTICATION messages.**

1740	49.638857	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58 Authentication, SN=1606, FN=0, Flags=........C
1741	49.639700	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58 Authentication, SN=1606, FN=0, Flags=....R...C
1742	49.640702	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58 Authentication, SN=1606, FN=0, Flags=....R...C
1744	49.642315	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58 Authentication, SN=1606, FN=0, Flags=....R...C
1746	49.645319	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58 Authentication, SN=1606, FN=0, Flags=....R...C
1749	49.649705	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58 Authentication, SN=1606, FN=0, Flags=....R...C
1821	53.785833	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58 Authentication, SN=1612, FN=0, Flags=........C
1822	53.787070	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58 Authentication, SN=1612, FN=0, Flags=....R...C
1921	57.889232	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58 Authentication, SN=1619, FN=0, Flags=........C
1922	57.890325	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58 Authentication, SN=1619, FN=0, Flags=....R...C
1923	57.891321	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58 Authentication, SN=1619, FN=0, Flags=....R...C
1924	57.896970	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58 Authentication, SN=1619, FN=0, Flags=....R...C
2122	62.171951	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58 Authentication, SN=1644, FN=0, Flags=........C
2123	62.172946	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58 Authentication, SN=1644, FN=0, Flags=....R...C
2124	62.174070	IntelCor_d1:b6:4f	Cisco-Li_f5:ba:bb	802.11	58 Authentication, SN=1644, FN=0, Flags=....R...C
2156	63.168087	IntelCor_d1:b6:4f	Cisco-Li_f7:1d:51	802.11	58 Authentication, SN=1647, FN=0, Flags=........C
2160	63.169707	IntelCor_d1:b6:4f	Cisco-Li_f7:1d:51	802.11	58 Authentication, SN=1647, FN=0, Flags=....R...C
2158	63.169071	Cisco-Li_f7:1d:51	IntelCor_d1:b6:4f	802.11	58 Authentication, SN=3726, FN=0, Flags=........C
2164	63.170692	Cisco-Li_f7:1d:51	IntelCor_d1:b6:4f	802.11	58 Authentication, SN=3727, FN=0, Flags=........C

11. Does the host want the authentication to require a key or be open?
A: Be open.

12. Do you see a reply AUTHENTICATION from the linksys_ses_24086 AP in the trace?
A: No. This is not an open AP, so the host is eventually unable to connect to this AP.

13. Now let's consider what happens as the host gives up trying to associate with the linksys_ses_24086 AP and now tries to associate with the 30 Munroe St AP. Look for AUTHENICATION frames sent from the host to and AP and vice versa. At what times are there an AUTHENTICATION frame from the host to the 30 Munroe St. AP, and when is there a reply AUTHENTICATION sent from that AP to the host in reply?

```
2156 63.168087 IntelCor_d1:b6:4f    Cisco-Li_f7:1d:51    802.11      58 Authentication, SN=1647, FN=0, Flags=........C
2160 63.169707 IntelCor_d1:b6:4f    Cisco-Li_f7:1d:51    802.11      58 Authentication, SN=1647, FN=0, Flags=....R...C
2158 63.169071 Cisco-Li_f7:1d:51    IntelCor_d1:b6:4f    802.11      58 Authentication, SN=3726, FN=0, Flags=........C
2164 63.170692 Cisco-Li_f7:1d:51    IntelCor_d1:b6:4f    802.11      58 Authentication, SN=3727, FN=0, Flags=........C
```

A: From host to AP: 63.168087, reply: 63.169071. From host to AP: 63.169707, reply: 63.170692.

14. An ASSOCIATE REQUEST from host to AP, and a corresponding ASSOCIATE RESPONSE frame from AP to host are used for the host to associate with an AP. At what time is there an ASSOCIATE REQUEST from host to the 30 Munroe St AP? When is the corresponding ASSOCIATE REPLY sent?

```
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
33.079714 d1:b6:4f:00:16:b6    MS-NLB-PhysServer-3… 802.11     111 Association Request, SN=3775, FN=4, Flags=.pm...F.C
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
63.192101 Cisco-Li_f7:1d:51    IntelCor_d1:b6:4f    802.11      94 Association Response, SN=3728, FN=0, Flags=........C
```

A: From host to AP: 63.169910, reply: 63.192101.

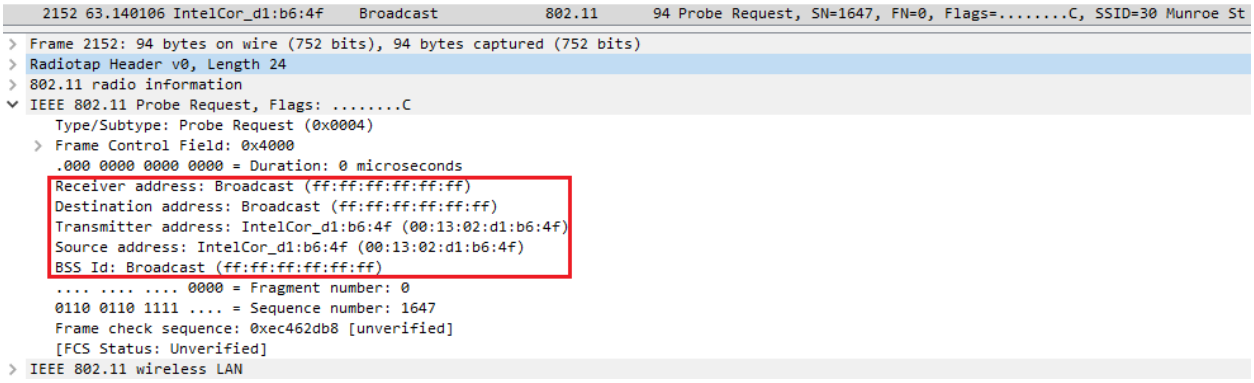
15. What transmission rates is the host willing to use? The AP? To answer this question, you will need to look into the parameter fields of the 802.11 wireless LAN management frame.

```
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
v IEEE 802.11 wireless LAN
  > Fixed parameters (4 bytes)
  v 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]
```

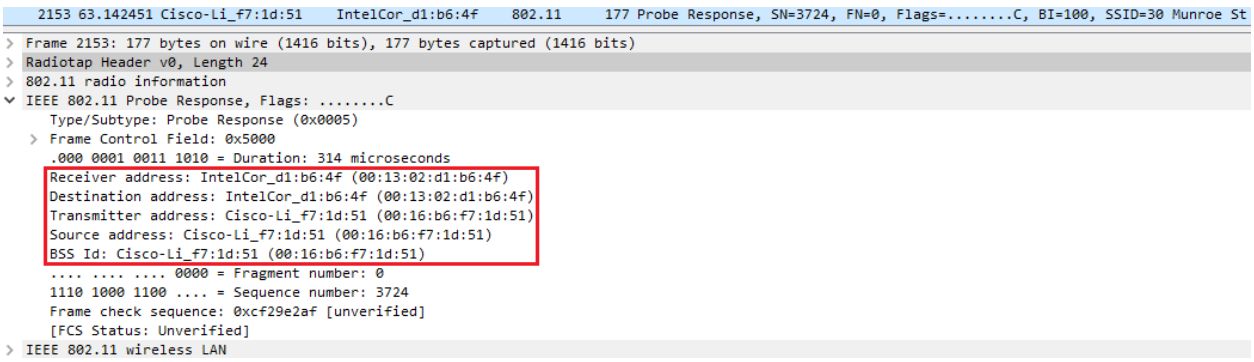
```
2166 63.192101 Cisco-Li_f7:1d:51    IntelCor_d1:b6:4f    802.11      94 Association Response, SN=3728, FN=0, Flags=........C
> Frame 2166: 94 bytes on wire (752 bits), 94 bytes captured (752 bits)
> Radiotap Header v0, Length 24
> 802.11 radio information
> IEEE 802.11 Association Response, Flags: ........C
v IEEE 802.11 wireless LAN
  > Fixed parameters (6 bytes)
  v 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
```

A: The host is willing to use 1, 2, 5.5, 11, 6, 9, 12, 18 (Mbps). Extended rates are 24, 36, 48, 54 (Mbps). The AP is willing to use 1, 2, 5.5, 11 (Mbps). Extended rates are 6, 9, 12, 18, 24, 36, 48, 54 (Mbps).

16. Our trace contains a number of PROBE REQUEST and PROBE RESPONSE frames. What are the sender, receiver and BSS ID MAC addresses in these frames? What is the purpose of these two types of frames?



A: MAC address: sender (00:13:02:d1:b6:4f), receiver (ff:ff:ff:ff:ff:ff), BSS ID (ff:ff:ff:ff:ff:ff).



A: MAC address: sender (00:16:b6:f7:1d:51), receiver (00:13:02:d1:b6:4f), BSS ID (00:16:b6:f7:1d:51).

The host broadcasts a Probe Request as active scanning. The AP replies with Probe Response.

Planning Wireless LAN Network Deployments Analysis

LAB 1: Mixed 11g/11n WLAN Performance

Objective: Determine impact of legacy 11g nodes on an 11n WLAN network.

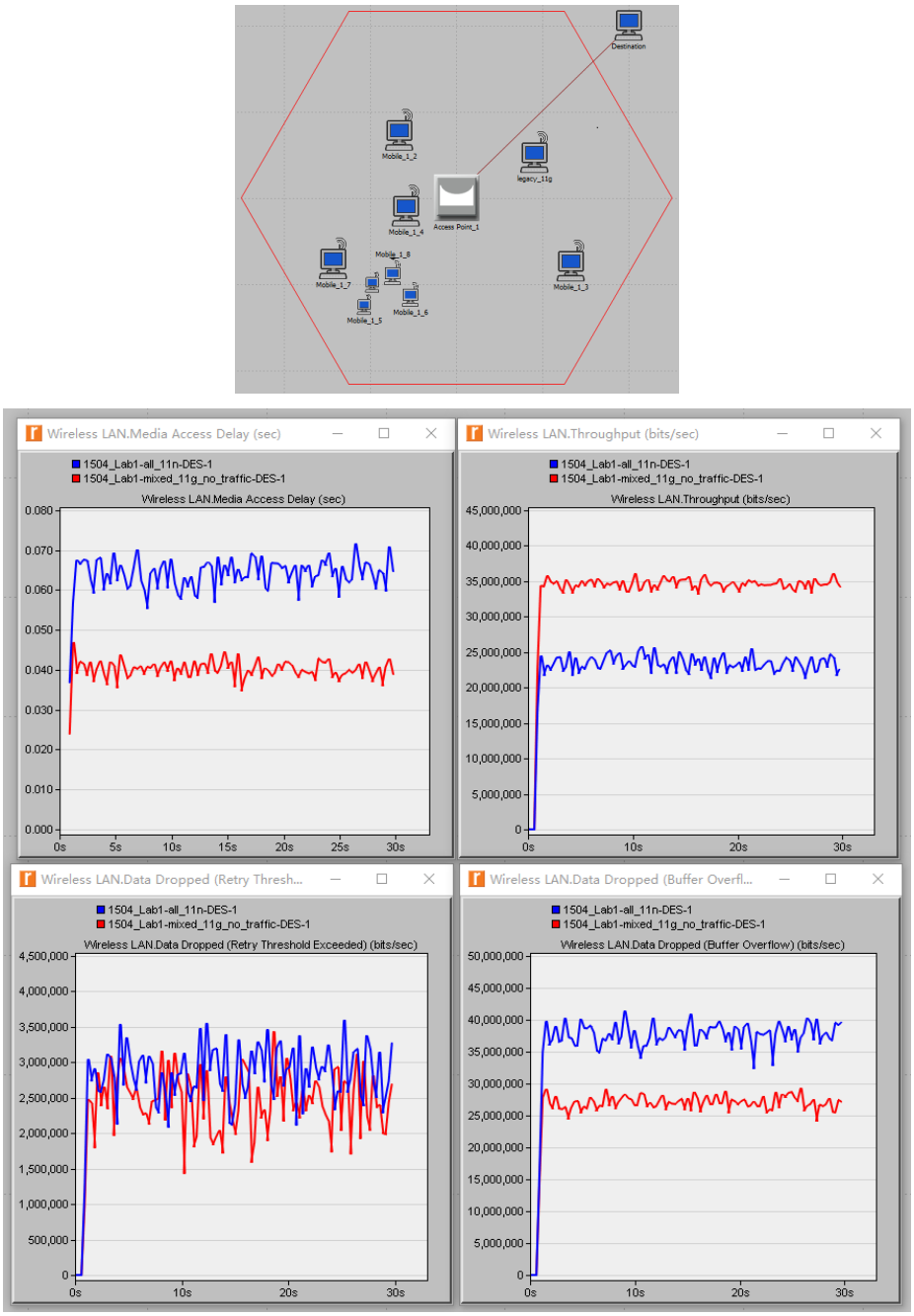


Figure 1 – Two Scenarios Comparison

Conclusion:
According to Figure 1(2), The throughput is improved with the introduce of legacy 11g nodes. Data Dropped (Retry Threshold Exceeded) has no difference, Data Dropped (Buffer Overflow) and Media Access Delay are less in 11g_no_traffic scenario.
CTS-to-Self Protection Mechanism improves the throughput due to fewer frames are sent.

LAB 2: Improving Performance with QoS Aware Wireless LAN Layer

Objective: Assess the performance of high-quality voice application together with HTTP application in an 11n infrastructure Wireless LAN BSS operating at 7.2 Mbps. Improve the performance of the network further by adjusting 802.11e parameters based on application load and topology conditions in the network.

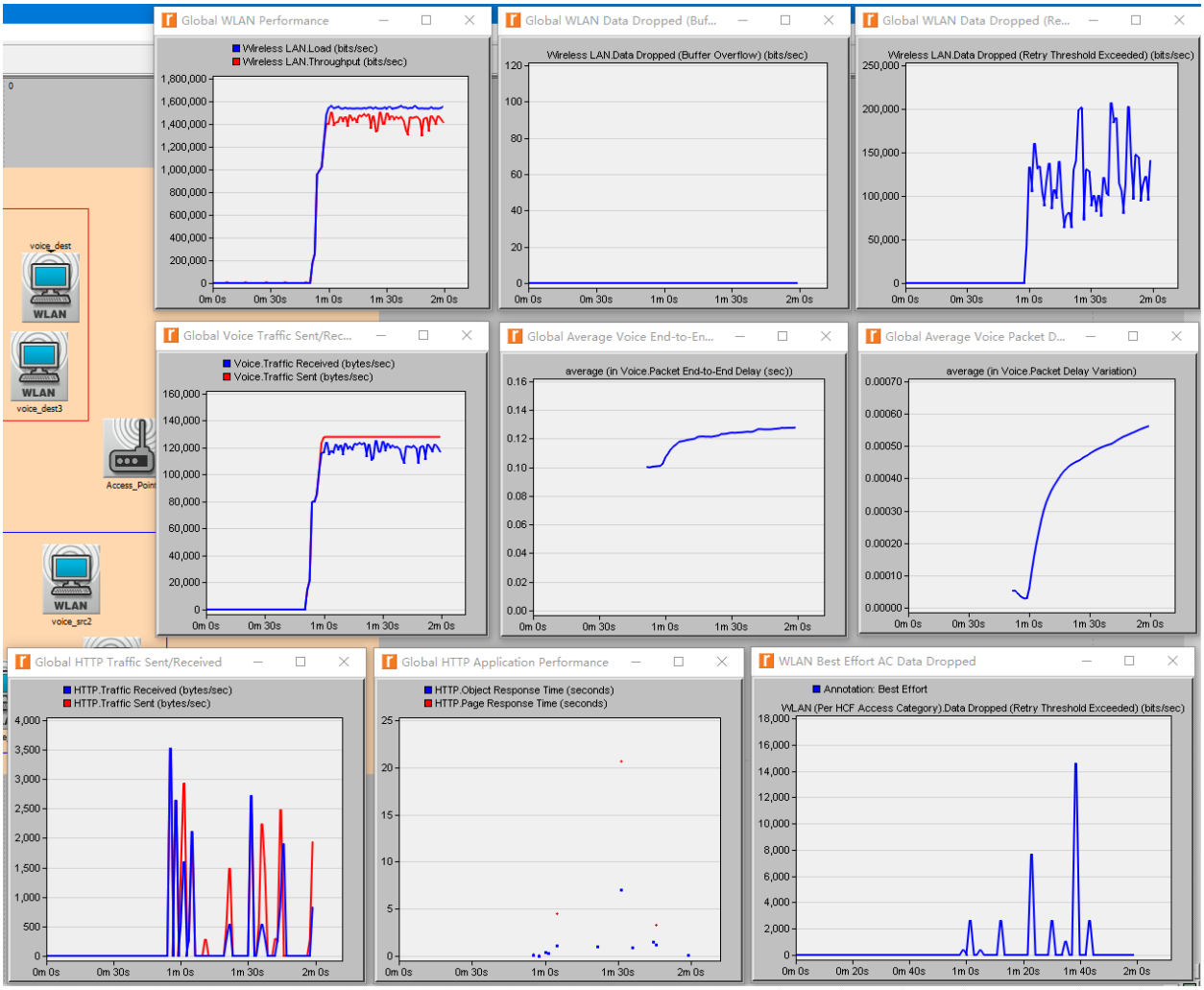


Figure 2 - Performance Observed at Application Layer with Default 11e Settings

Conclusion:

No data dropped due to Buffer Overflow, many are dropped due to Retry Threshold Exceeded.

There are some losses and short delays in voice application.

The HTTP Performance is not so good considering only ten or more pages and objects are downloaded.

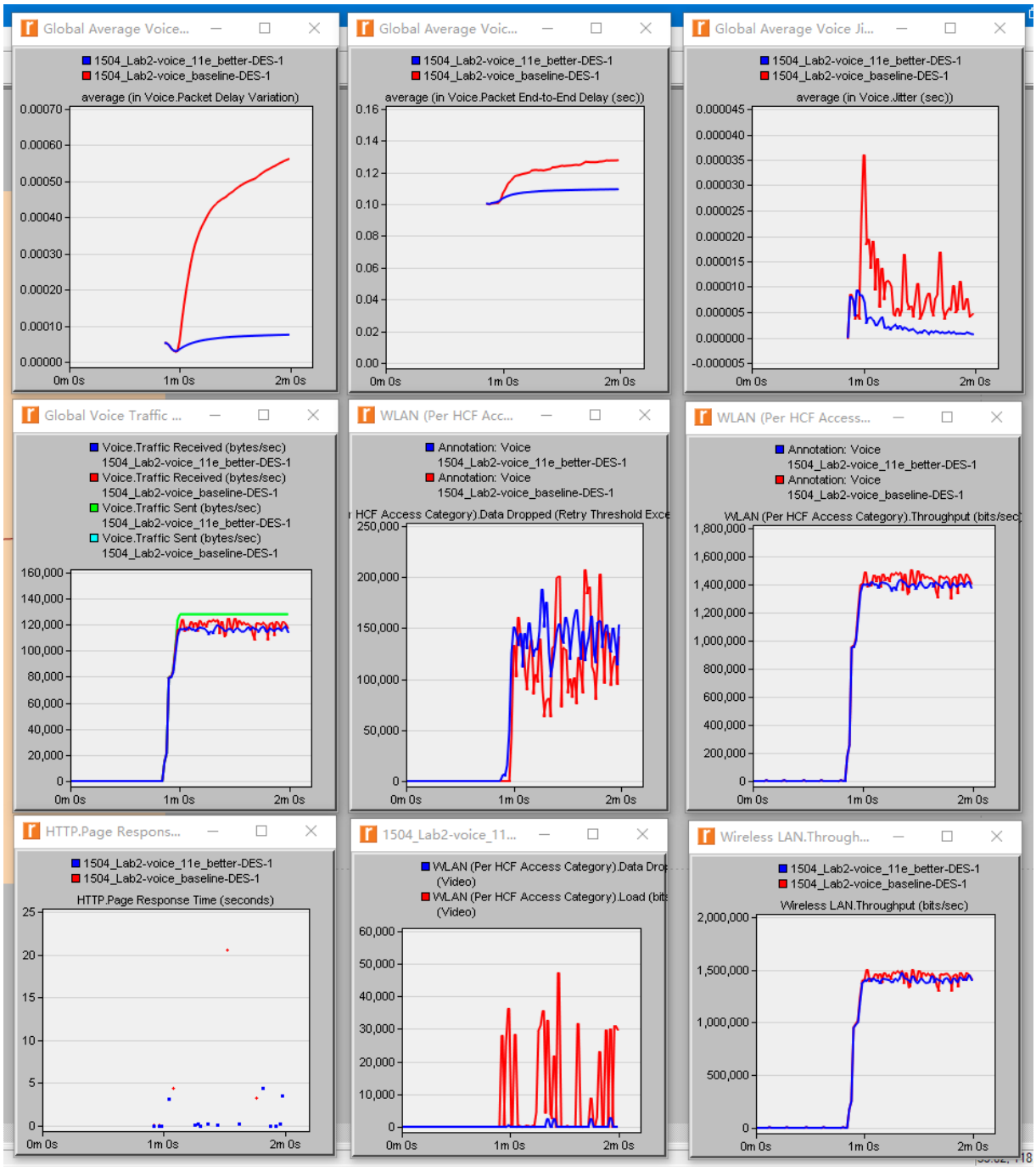


Figure 3 – Comparison after Performance Tuning for 11e Network

Conclusion:
The delay in voice application are improved significantly.
However, there is less difference in Voice AC dropped data and throughput.
The HTTP Performance improved a little though it is mapped to a higher priority Access Category.
The Wireless LAN Throughput is also very similar.

Conclusion

This lab is mainly focused on IEEE 802.11.
In the Wireshark part, beacon frames, addresses and other details are analyzed.
In the Riverbed part, WLAN models are used to introduce some ways which can improve network performances.
Some results have reached expectation.
However, in the last part of the Riverbed lab, the simulation doesn't show a significant improvement in network performance.

Nov.9 2019