# Lab4: Wireshark Analysis and Riverbed Modeling of WLANs

## EE450

## Session 2


## Yin-Hsia Yen

# Abstract

This lab consists of two separate labs that examines the interactions between hosts under internet environment.

The first lab, Wireshark Analysis of IEEE802.11, examines the behavior of frames and packets transmit between a wireless host to the first-hop-router through beacon frames, TCP protocols, and other related protocols. The focus on this lab is to identify the MAC and IP address of each device.

The second lab, Planning Wireless LAN Network Deployments, also consists of two mini labs. The first mini lab examines the impact of legacy 802.11g nodes on an 802.11n WLAN network. The second mini lab examines differences in network performance effects by adjusting network parameters.

# Part1. Wireshark Analysis of IEEE802.11

Based on Wireshark_802_11.pcap trace file

Q1. What are the SSIDs of the two access points that are issuing most of the beacon frames in this trace?

SSID: **30 Munroe St** & SSID: **linksys12** issued most of the beacon frames.

| | | | | | | |
|---|---|---|---|---|---|---|
| 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 |
| 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 |
| 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=li\357\277\275\001\004 |
| 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 |
| 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 |
| 15 | 0.597382 | Cisco-Li_f7:1d:51 | Broadcast | 802.11 | 183 | Beacon frame, SN=2860, FN=0, Flags=........C, BI=100, SSID=30 Munroe St |
| 16 | 0.601687 | LinksysG_67:22:94 | Broadcast | 802.11 | 90 | Beacon frame, SN=3075, FN=0, Flags=........C, BI=100, SSID=linksys12 |
| 17 | 0.699847 | Cisco-Li_f7:1d:51 | Broadcast | 802.11 | 183 | Beacon frame, SN=2861, FN=0, Flags=........C, BI=100, SSID=30 Munroe St |
| 18 | 0.802226 | Cisco-Li_f7:1d:51 | Broadcast | 802.11 | 183 | Beacon frame, SN=2862, FN=0, Flags=........C, BI=100, SSID=30 Munroe St |
| 19 | 0.904619 | Cisco-Li_f7:1d:51 | Broadcast | 802.11 | 183 | Beacon frame, SN=2863, FN=0, Flags=........C, BI=100, SSID=30 Munroe St |
| 20 | 1.007015 | Cisco-Li_f7:1d:51 | Broadcast | 802.11 | 183 | Beacon frame, SN=2864, FN=0, Flags=........C, BI=100, SSID=30 Munroe St |
| 21 | 1.010949 | LinksysG_67:22:94 | Broadcast | 802.11 | 90 | Beacon frame, SN=3079, FN=0, Flags=........C, BI=100, SSID=linksys12 |
| 22 | 1.109406 | Cisco-Li_f7:1d:51 | Broadcast | 802.11 | 183 | Beacon frame, SN=2865, FN=0, Flags=........C, BI=100, SSID=30 Munroe St |
| 23 | 1.113691 | LinksysG_67:22:94 | Broadcast | 802.11 | 90 | Beacon frame, SN=3080, FN=0, Flags=........C, BI=100, SSID=,\357\277\275nksys |
| 24 | 1.211843 | Cisco-Li_f7:1d:51 | Broadcast | 802.11 | 183 | Beacon frame, SN=2866, FN=0, Flags=........C, BI=100, SSID=30 Munroe St |
| 27 | 1.212185 | Cisco-Li_f7:1d:51 | IntelCor_d1:b6:4f | 802.11 | 177 | Probe Response, SN=2867, FN=0, Flags=........C, BI=100, SSID=30 Munroe St |
| 31 | 1.215947 | LinksysG_67:22:94 | Broadcast | 802.11 | 90 | Beacon frame, SN=3081, FN=0, Flags=........C, BI=100, SSID=linksys12 |
| 32 | 1.314223 | Cisco-Li_f7:1d:51 | Broadcast | 802.11 | 183 | Beacon frame, SN=2868, FN=0, Flags=........C, BI=100, SSID=30 Munroe St |
| 33 | 1.416593 | Cisco-Li_f7:1d:51 | Broadcast | 802.11 | 183 | Beacon frame, SN=2869, FN=0, Flags=........C, BI=100, SSID=30 Munroe St |
| 34 | 1.420565 | LinksysG_67:22:94 | Broadcast | 802.11 | 90 | Beacon frame, SN=3083, FN=0, Flags=........C, BI=20580, SSID=linksys12 |
| 35 | 1.519009 | Cisco-Li_f7:1d:51 | Broadcast | 802.11 | 183 | Beacon frame, SN=2870, FN=0, Flags=........C, BI=100, SSID=30 Munroe St |
| 36 | 1.621422 | Cisco-Li_f7:1d:51 | Broadcast | 802.11 | 183 | Beacon frame, SN=2871, FN=0, Flags=........C, BI=100, SSID=30 Munroe St |
| 37 | 1.724031 | Cisco-Li_f7:1d:51 | Broadcast | 802.11 | 183 | Beacon frame, SN=2872, FN=0, Flags=........C, BI=100, SSID=30 Munroe St |

Q2. 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?

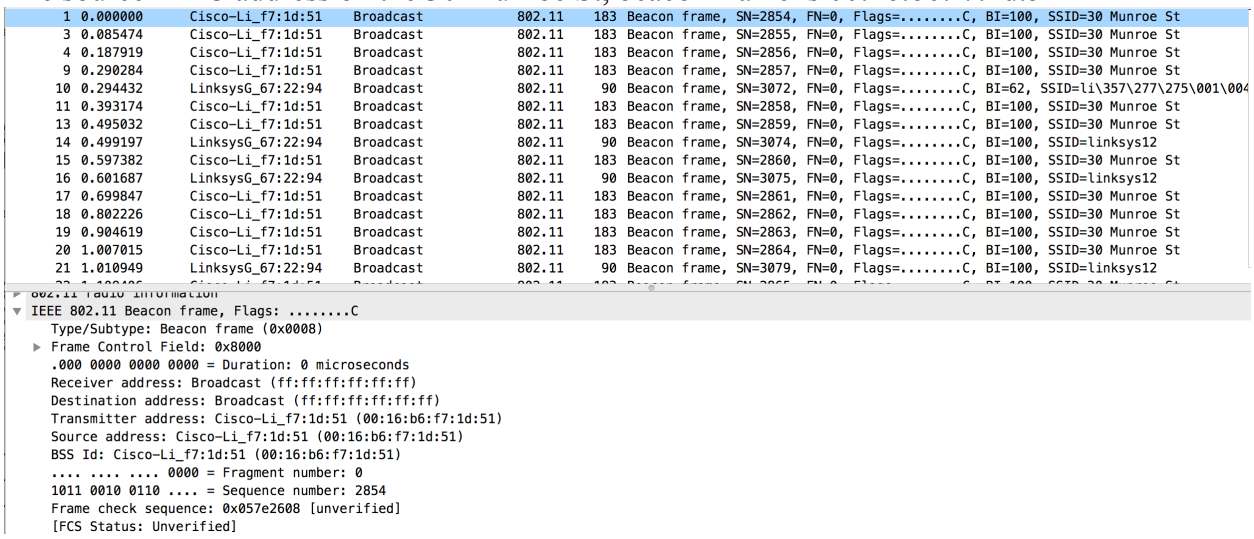
The beacon interval for both access points is 0.1024 seconds. The beacon frames from *30 Munroe St*. in the trace shown up regularly, however, the beacon frames from *linksys_ses_24086* do not.

| | | | | | | |
|---|---|---|---|---|---|---|
| 2312 | 70.533706 | Cisco-Li_f7:1d:51 | Broadcast | 802.11 | 183 | Beacon frame, SN=3805, FN=0, Flags=........C, BI=100, SSID=30 Munroe St |
| 2313 | 70.635970 | Cisco-Li_f7:1d:51 | Broadcast | 802.11 | 183 | Beacon frame, SN=3806, FN=0, Flags=........C, BI=100, SSID=30 Munroe St |
| 2314 | 70.738327 | Cisco-Li_f7:1d:51 | Broadcast | 802.11 | 183 | Beacon frame, SN=3807, FN=0, Flags=........C, BI=100, SSID=30 Munroe St |
| 2315 | 70.840739 | Cisco-Li_f7:1d:51 | Broadcast | 802.11 | 183 | Beacon frame, SN=3808, FN=0, Flags=........C, BI=100, SSID=30 Munroe St |
| 2319 | 70.943156 | Cisco-Li_f7:1d:51 | Broadcast | 802.11 | 183 | Beacon frame, SN=3809, FN=0, Flags=........C, BI=100, SSID=30 Munroe St |
| 2320 | 71.045542 | Cisco-Li_f7:1d:51 | Broadcast | 802.11 | 183 | Beacon frame, SN=3810, FN=0, Flags=........C, BI=100, SSID=30 Munroe St |
| 2321 | 71.101576 | Cisco-Li_f5:ba:bb | Broadcast | 802.11 | 132 | Beacon frame, SN=3954, FN=0, Flags=........C, BI=100, SSID=linksys_SES_24086 |
| 2322 | 71.147898 | Cisco-Li_f7:1d:51 | Broadcast | 802.11 | 183 | Beacon frame, SN=3811, FN=0, Flags=........C, BI=100, SSID=30 Munroe St |
| 2323 | 71.250339 | Cisco-Li_f7:1d:51 | Broadcast | 802.11 | 183 | Beacon frame, SN=3812, FN=0, Flags=........C, BI=100, SSID=30 Munroe St |
| 2327 | 71.352708 | Cisco-Li_f7:1d:51 | Broadcast | 802.11 | 183 | Beacon frame, SN=3813, FN=0, Flags=........C, BI=100, SSID=30 Munroe St |
| 2328 | 71.455065 | Cisco-Li_f7:1d:51 | Broadcast | 802.11 | 183 | Beacon frame, SN=3814, FN=0, Flags=........C, BI=100, SSID=30 Munroe St |
| 2331 | 71.557330 | Cisco-Li_f7:1d:51 | Broadcast | 802.11 | 183 | Beacon frame, SN=3815, FN=0, Flags=........C, BI=100, SSID=30 Munroe St |
| 2334 | 71.659897 | Cisco-Li_f7:1d:51 | Broadcast | 802.11 | 183 | Beacon frame, SN=3816, FN=0, Flags=........C, BI=100, SSID=30 Munroe St |
| 2336 | 71.762287 | Cisco-Li_f7:1d:51 | Broadcast | 802.11 | 183 | Beacon frame, SN=3817, FN=0, Flags=........C, BI=100, SSID=30 Munroe St |
| 2337 | 71.864626 | Cisco-Li_f7:1d:51 | Broadcast | 802.11 | 183 | Beacon frame, SN=3818, FN=0, Flags=........C, BI=100, SSID=30 Munroe St |
| 2338 | 71.967102 | Cisco-Li_f7:1d:51 | Broadcast | 802.11 | 183 | Beacon frame, SN=3819, FN=0, Flags=........C, BI=100, SSID=30 Munroe St |

```
▼ IEEE 802.11 wireless LAN
  ▼ Fixed parameters (12 bytes)
      Timestamp: 6351992627604
      Beacon Interval: 0.102400 [Seconds]
    ▶ Capabilities Information: 0x0011
  ▼ Tagged parameters (68 bytes)
    ▼ Tag: SSID parameter set: linksys_SES_24086
        Tag Number: SSID parameter set (0)
        Tag length: 17
        SSID: linksys_SES_24086
    ▼ 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)
```

Q3. What (in hexadecimal notation) is the source MAC address on the beacon frame from *30 Munroe St*?

The source MAC address on the 30 Munroe St, beacon frame is 00:16:b6:f7:1d:51




Q4. What (in hexadecimal notation) is the destination MAC address on the beacon frame from *30 Munroe St*?

Reference picture from Q3.

The destination MAC address on the 30 Munroe St, beacon frame is ff:ff:ff:ff:ff:ff (Ethernet broadcast address).

Q5. What (in hexadecimal notation) is the MAC BSS id on the beacon frame from *30 Munroe St*?

Reference picture from Q3.

The MAC BSS ID address on the 30 Munroe St, beacon frame is 00:16:b6:f7:1d:51 (the same as for the source address).

Q6. 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?

The support rates are 1.0, 2.0, 5.5, 11.0 Mbps. The extended rates are 6.0, 9.0, 12.0, 18.0, 24.0, 36.0, 48.0 and 54.0 Mbps.

```
▼ Fixed parameters (12 bytes)
    Timestamp: 174319001986
    Beacon Interval: 0.102400 [Seconds]
  ▶ Capabilities Information: 0x0601
▼ Tagged parameters (119 bytes)
  ▶ Tag: SSID parameter set: 30 Munroe St
  ▶ Tag: Supported Rates 1(B), 2(B), 5.5(B), 11(B), [Mbit/sec]
  ▶ Tag: DS Parameter set: Current Channel: 6
  ▶ Tag: Traffic Indication Map (TIM): DTIM 0 of 0 bitmap
  ▶ Tag: Country Information: Country Code US, Environment Indoor
  ▶ Tag: EDCA Parameter Set
  ▶ Tag: ERP Information
  ▶ Tag: Extended Supported Rates 6(B), 9, 12(B), 18, 24(B), 36, 48, 54, [Mbit/sec]
  ▶ Tag: Vendor Specific: Airgo Networks, Inc.
  ▶ Tag: Vendor Specific: Microsoft Corp.: WMM/WME: Parameter Element
```

Q7. 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.

The TCP SYN is sent at t = 24.811093 seconds.
The MAC address for the host (the source MAC address) is 00:13:02:d1:b6:4f.
The MAC address for the destination (the first hop router/ the access point) is 00:16:b6:f4:eb:a8.
The MAC address for the BSS is 00:16:b6:f7:1d:51.
The IP address of the host is 192.168.1.109
The destination IP address is 128.199.245.12 (the IP address of gaia.cs.umass.edu).

To sum up, the source MAC and IP is the MAC and IP of the host it self, and the destination MAC is the first-hop router, and destination IP is the IP of the destination it sends TCP segment to.

```
470 24.795673   192.168.1.109   68.87.71.226      DNS       125 Standard query 0x7892 A gaia.cs.umass.edu
471 24.795769                   IntelCor_d1:b6:4f … 802.11    38 Acknowledgement, Flags=........C
472 24.809325   68.87.71.226    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 … 802.11    38 Acknowledgement, Flags=........C
474 24.811093   192.168.1.109   128.119.245.12    TCP       110 2538 → 80 [SYN] Seq=0 Win=16384 Len=0 MSS=1460 SACK_PERM=1
475 24.811231                   IntelCor_d1:b6:4f … 802.11    38 Acknowledgement, Flags=........C
476 24.827751   128.119.245.12  192.168.1.109     TCP       110 80 → 2538 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 SACK_PERM=1
477 24.827922                   Cisco-Li_f7:1d:51 … 802.11    38 Acknowledgement, Flags=........C
478 24.828024   192.168.1.109   128.119.245.12    TCP       102 2538 → 80 [ACK] Seq=1 Ack=1 Win=17520 Len=0
479 24.828140                   IntelCor_d1:b6:4f … 802.11    38 Acknowledgement, Flags=........C
480 24.828253   192.168.1.109   128.119.245.12    HTTP      537 GET /wireshark-labs/alice.txt HTTP/1.1
481 24.828352                   IntelCor_d1:b6:4f … 802.11    38 Acknowledgement, Flags=........C
482 24.846898   128.119.245.12  192.168.1.109     TCP       108 80 → 2538 [ACK] Seq=1 Ack=436 Win=6432 Len=0
483 24.847058                   Cisco-Li_f7:1d:51 … 802.11    38 Acknowledgement, Flags=........C
484 24.847171   128.119.245.12  192.168.1.109     TCP       108 [TCP Dup ACK 482#1] 80 → 2538 [ACK] Seq=1 Ack=436 Win=6432 Len=0

▶ Frame 474: 110 bytes on wire (880 bits), 110 bytes captured (880 bits)
▶ Radiotap Header v0, Length 24
▶ 802.11 radio information
▼ IEEE 802.11 QoS Data, Flags: .......TC
    Type/Subtype: QoS Data (0x0028)
  ▶ Frame Control Field: 0x8801
    .000 0000 0010 1100 = Duration: 44 microseconds
    Receiver address: Cisco-Li_f7:1d:51 (00:16:b6:f7:1d:51)
    Transmitter address: IntelCor_d1:b6:4f (00:13:02:d1:b6:4f)
    Destination address: Cisco-Li_f4:eb:a8 (00:16:b6:f4:eb:a8)
    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)
    STA address: IntelCor_d1:b6:4f (00:13:02:d1:b6:4f)
    .... .... .... 0000 = Fragment number: 0
    0000 0011 0001 .... = Sequence number: 49
```

```
▼ Internet Protocol Version 4, Src: 192.168.1.109, Dst: 128.119.245.12
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  ▶ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 48
    Identification: 0x1324 (4900)
  ▶ Flags: 0x4000, Don't fragment
    Time to live: 128
    Protocol: TCP (6)
    Header checksum: 0xb00a [validation disabled]
    [Header checksum status: Unverified]
    Source: 192.168.1.109
    Destination: 128.119.245.12
```

Q8. 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?

The TCP SYNACK is received at t = 24.827751 seconds
The MAC address for the sender (the 1st hop router/ the access point) is 00:16:b6:f4:eb:a8
The MAC address for the destination (the host) is 91:2a:b0:49:b6:4f

Observed from previous question, it is different from the MAC address of the host used in the frame that sends the TCP SYN, which means the host wireless interface is behaving as if it has two interface addresses

The MAC address for the BSS is 00:16:b6:f7:1d:51
The IP address of the server sending the TCP SYNACK is 128.199.245.12 (gaia.cs.umass.edu)
The destination address is 192.168.1.109

```
▶ Frame 476: 110 bytes on wire (880 bits), 110 bytes captured (880 bits)
▶ Radiotap Header v0, Length 24
▶ 802.11 radio information
▼ IEEE 802.11 QoS Data, Flags: ..mP..F.C
    Type/Subtype: QoS Data (0x0028)
  ▶ Frame Control Field: 0x8832
    Duration/ID: 11560 (reserved)
    Receiver address: 91:2a:b0:49:b6:4f (91:2a:b0:49:b6:4f)
    Transmitter address: Cisco-Li_f7:1d:51 (00:16:b6:f7:1d:51)
    Destination address: 91:2a:b0:49:b6:4f (91:2a:b0:49:b6:4f)
    Source address: Cisco-Li_f4:eb:a8 (00:16:b6:f4:eb:a8)
    BSS Id: Cisco-Li_f7:1d:51 (00:16:b6:f7:1d:51)
    STA address: 91:2a:b0:49:b6:4f (91:2a:b0:49:b6:4f)
    .... .... .... 0000 = Fragment number: 0
    1100 0011 0100 .... = Sequence number: 3124
    Frame check sequence: 0xecdc407d [unverified]
    [FCS Status: Unverified]
```

```
▼ Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.109
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  ▶ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 48
    Identification: 0x0000 (0)
  ▶ Flags: 0x4000, Don't fragment
    Time to live: 49
    Protocol: TCP (6)
    Header checksum: 0x122f [validation disabled]
    [Header checksum status: Unverified]
    Source: 128.119.245.12
    Destination: 192.168.1.109
```

Q9. 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? Looking at the 802.11 specification, is there another frame that you might have expected to see, but don't see here?

At t = 49.583615 (Frame 1733), DHCP server sends out a DHCP release

At t = 49.609617 (Frame 1735), the host sends a DEAUTHENTICATION frame.

One might have expected to see is a DISASSOCIATION request

| No. | Time | Source | Destination | Protocol | Length | Info |
|---|---|---|---|---|---|---|
| 1729 | 49.440041 | Cisco-Li_f7:1d:51 | Broadcast | 802.11 | 183 | Beacon frame, SN=3587, FN=0, Flags=........C, BI=100, SSID=30 Munroe St |
| 1730 | 49.440146 | IntelCor_d1:b6:4f | Cisco-Li_f7:1d:51 | 802.11 | 54 | QoS Null function (No data), SN=1604, FN=0, Flags=...P...TC |
| 1731 | 49.440243 | | IntelCor_d1:b6:4f … | 802.11 | 38 | Acknowledgement, Flags=........C |
| 1732 | 49.542481 | Cisco-Li_f7:1d:51 | Broadcast | 802.11 | 183 | Beacon frame, SN=3588, FN=0, Flags=........C, BI=100, SSID=30 Munroe St |
| 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 |

Q10. 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?*

At t = 49.638857 (Frame 1740), the first AUTHENTICATION message sent from the host to the access point.

| No. | Time | Source | Destination | Protocol | Length | Info |
|---|---|---|---|---|---|---|
| 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 |
| 1745 | 49.644710 | Cisco-Li_f7:1d:51 | Broadcast | 802.11 | 183 | Beacon frame, SN=3589, FN=0, Flags=........C, BI=100, SSID=30 Munroe St |
| 1746 | 49.645319 | IntelCor_d1:b6:4f | Cisco-Li_f5:ba:bb | 802.11 | 58 | Authentication, SN=1606, FN=0, Flags=....R...C |
| 1747 | 49.646711 | | Cisco-Li_f5:ba:bb … | 802.11 | 38 | Acknowledgement, Flags=........C |
| 1748 | 49.647827 | | Cisco-Li_f5:ba:bb … | 802.11 | 38 | Acknowledgement, Flags=........C |

Q11. Does the host want the authentication to require a key or be open?

The host is requesting that the association be open

```
▶ Frame 1740: 58 bytes on wire (464 bits), 58 bytes captured (464 bits)
▶ Radiotap Header v0, Length 24
▶ 802.11 radio information
▶ IEEE 802.11 Authentication, Flags: ........C
▼ IEEE 802.11 wireless LAN
  ▼ Fixed parameters (6 bytes)
      Authentication Algorithm: Open System (0)
      Authentication SEQ: 0x0001
      Status code: Successful (0x0000)
```

Q12. Do you see a reply AUTHENTICATION from the *linksys_ses_24086* AP in the trace?

No, can't find any reply from the AP

Q13. 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?

At t = 63.168087 (Frame 2156), an AUTHENTICATION frame sent from the wireless host to the BSS.
At t = 63.169071 (Frame 2158), an AUTHENTICATION frame sent from the BSS to the wireless host.

| No. | Time | Source | Destination | Protocol | Length | Info |
|---|---|---|---|---|---|---|
| 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 |
| 2158 | 63.169071 | Cisco-Li_f7:1d:51 | IntelCor_d1:b6:4f | 802.11 | 58 | Authentication, SN=3726, 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 |
| 2164 | 63.170692 | Cisco-Li_f7:1d:51 | IntelCor_d1:b6:4f | 802.11 | 58 | Authentication, SN=3727, FN=0, Flags=........C |

Q14. An ASSOCIATE REQUEST from host to AP, and a corresponding ASSOCIATE RESPONSE frame from AP to host are used for the host to associated 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?

At t = 63.169910 (Frame 2162), an ASSOCIATE REQUEST frame sent from the wireless host to the BSS.
At t = 63.192101 (Frame 2166), an ASSOCIATE RESPONSE frame sent from the BSS to the wireless host.

| No. | Time | Source | Destination | Protocol | Length | Info |
|---|---|---|---|---|---|---|
| 1827 | 53.793568 | IntelCor_d1:b6:4f | Cisco-Li_f5:ba:bb | 802.11 | 107 | Association Request, SN=1613, FN=0, Flags=........C, SSID=linksys_SES_24086 |
| 1926 | 57.903699 | IntelCor_d1:b6:4f | Cisco-Li_f5:ba:bb | 802.11 | 107 | Association Request, SN=1620, FN=0, Flags=........C, SSID=linksys_SES_24086 |
| 1927 | 57.904945 | IntelCor_d1:b6:4f | Cisco-Li_f5:ba:bb | 802.11 | 107 | Association Request, SN=1620, FN=0, Flags=....R...C, SSID=linksys_SES_24086 |
| 1932 | 57.911195 | IntelCor_d1:b6:4f | Cisco-Li_f5:ba:bb | 802.11 | 107 | Association Request, SN=1620, FN=0, Flags=....R...C, SSID=linksys_SES_24086 |
| 1933 | 57.915945 | IntelCor_d1:b6:4f | Cisco-Li_f5:ba:bb | 802.11 | 107 | Association Request, SN=1620, FN=0, Flags=....R...C, SSID=linksys_SES_24086 |
| 1934 | 57.924199 | IntelCor_d1:b6:4f | Cisco-Li_f5:ba:bb | 802.11 | 107 | Association Request, SN=1620, FN=0, Flags=....R...C, SSID=linksys_SES_24086 |
| 1935 | 57.936216 | IntelCor_d1:b6:4f | Cisco-Li_f5:ba:bb | 802.11 | 107 | Association Request, SN=1620, FN=0, Flags=....R...C, SSID=linksys_SES_24086 |
| 1937 | 57.939196 | IntelCor_d1:b6:4f | Cisco-Li_f5:ba:bb | 802.11 | 107 | Association Request, SN=1620, FN=0, Flags=........C, SSID=linksys_SES_24086 |
| 2126 | 62.176945 | IntelCor_d1:b6:4f | Cisco-Li_f5:ba:bb | 802.11 | 107 | Association Request, SN=1645, FN=0, Flags=........C, SSID=linksys_SES_24086 |
| 2127 | 62.178194 | IntelCor_d1:b6:4f | Cisco-Li_f5:ba:bb | 802.11 | 107 | Association Request, SN=1645, FN=0, Flags=....R...C, SSID=linksys_SES_24086 |
| 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 |
| 2166 | 63.192101 | Cisco-Li_f7:1d:51 | IntelCor_d1:b6:4f | 802.11 | 94 | Association Response, SN=3728, FN=0, Flags=........C |
| 2307 | 70.179949 | Cisco-Li_f5:ba:7b | f9:ff:ff:ff:ff:ff | 802.11 | 132 | Fragmented IEEE 802.11 frame |

Q15. What transmission rates is the host willing to use? The AP?

The transmission rates the host willing to use are **1, 2, 5.5, 11, 6, 9, 12, 18, 24, 32, 48,** and **54** Mbps in the ASSOCIATION REQUEST and ASSOCIATION RESPONSE frames.

Q16. 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?

At t = 2.297613 (Frame 50), a PROBE REQUEST was sent from 00:12:f0:1f:57:13 to broadcast with a BSS ID of ff:ff:ff:ff:ff:ff as well.
At t = 2.300697 (Frame 51), a PROBE RESPONSE was sent from 00:16:b6:f7:1d:51 to a BSS ID of 00:16:b6:f7:1d:51.
A PROBE REQUEST is used by a host in active scanning to find an Access Point. A PROBE RESPONSE is sent by the access point to the host sending the request.

| No. | Time | Source | Destination | Protocol | Length | Info |
|---|---|---|---|---|---|---|
| 46 | 2.236634 | IntelCor_d1:b6:4f | Cisco-Li_f7:1d:51 | 802.11 | 54 | QoS Null function (No data), SN=1486, FN=0, Flags=.......TC |
| 47 | 2.236730 | | IntelCor_d1:b6:4f … | 802.11 | 38 | Acknowledgement, Flags=........C |
| 48 | 2.237689 | IntelCor_d1:b6:4f | Cisco-Li_f7:1d:51 | 802.11 | 54 | QoS Null function (No data), SN=1487, FN=0, Flags=...P...TC |
| 49 | 2.237786 | | IntelCor_d1:b6:4f … | 802.11 | 38 | Acknowledgement, Flags=........C |
| 50 | 2.297613 | IntelCor_1f:57:13 | Broadcast | 802.11 | 79 | Probe Request, SN=576, FN=0, Flags=........C, SSID=Home WIFI |
| 51 | 2.300697 | Cisco-Li_f7:1d:51 | IntelCor_1f:57:13 | 802.11 | 177 | Probe Response, SN=2878, FN=0, Flags=........C, BI=100, SSID=30 Munroe St |
| 52 | 2.302191 | Cisco-Li_f7:1d:51 | IntelCor_1f:57:13 | 802.11 | 177 | Probe Response, SN=2878, FN=0, Flags=....R...C, BI=100, SSID=30 Munroe St |
| 53 | 2.304063 | Cisco-Li_f7:1d:51 | IntelCor_1f:57:13 | 802.11 | 177 | Probe Response, SN=2878, FN=0, Flags=....R...C, BI=100, SSID=30 Munroe St |
| 54 | 2.305562 | Cisco-Li_f7:1d:51 | IntelCor_1f:57:13 | 802.11 | 177 | Probe Response, SN=2878, FN=0, Flags=....R...C, BI=100, SSID=30 Munroe St |
| 55 | 2.308563 | Cisco-Li_f7:1d:51 | IntelCor_1f:57:13 | 802.11 | 177 | Probe Response, SN=2878, FN=0, Flags=....R...C, BI=100, SSID=30 Munroe St |
| 56 | 2.310072 | Cisco-Li_f7:1d:51 | IntelCor_1f:57:13 | 802.11 | 177 | Probe Response, SN=2878, FN=0, Flags=....R...C, BI=100, SSID=30 Munroe St |
| 57 | 2.338148 | Cisco-Li_f7:1d:51 | Broadcast | 802.11 | 183 | Beacon frame, SN=2879, FN=0, Flags=........C, BI=100, SSID=30 Munroe St |
| 58 | 2.440572 | Cisco-Li_f7:1d:51 | Broadcast | 802.11 | 183 | Beacon frame, SN=2880, FN=0, Flags=........C, BI=100, SSID=30 Munroe St |
| 59 | 2.453941 | Cisco-Li_f7:1d:51 | IntelCor_1f:57:13 | 802.11 | 177 | Probe Response, SN=2881, FN=0, Flags=........C, BI=100, SSID=30 Munroe St |

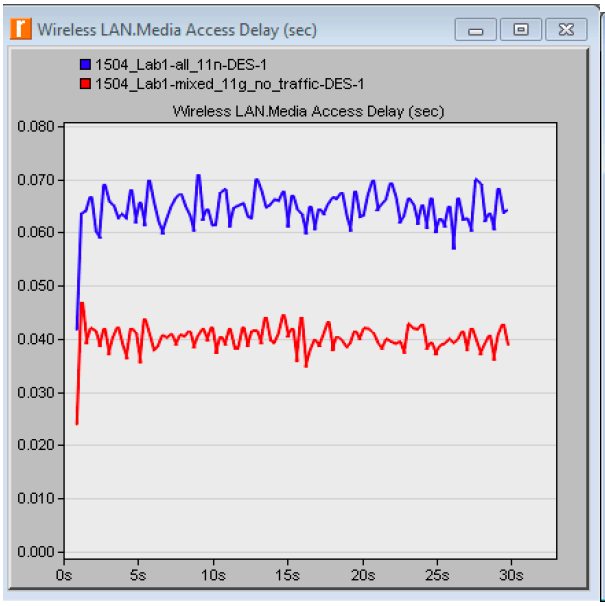
```
▶ Frame 50: 79 bytes on wire (632 bits), 79 bytes captured (632 bits)
▶ Radiotap Header v0, Length 24
▶ 802.11 radio information
▼ IEEE 802.11 Probe Request, Flags: ........C
    Type/Subtype: Probe Request (0x0004)
  ▶ Frame Control Field: 0x4000
    .000 0000 0000 0000 = Duration: 0 microseconds
    Receiver address: Broadcast (ff:ff:ff:ff:ff:ff)
    Destination address: Broadcast (ff:ff:ff:ff:ff:ff)
    Transmitter address: 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]
```

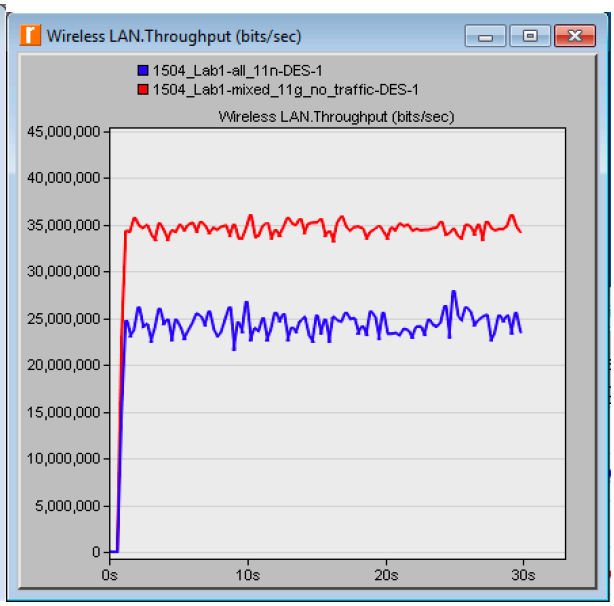
```
▶ Frame 51: 177 bytes on wire (1416 bits), 177 bytes captured (1416 bits)
▶ Radiotap Header v0, Length 24
▶ 802.11 radio information
▼ IEEE 802.11 Probe Response, Flags: ........C
    Type/Subtype: Probe Response (0x0005)
  ▶ Frame Control Field: 0x5000
    .000 0001 0011 1010 = Duration: 314 microseconds
    Receiver address: IntelCor_1f:57:13 (00:12:f0:1f:57:13)
    Destination address: IntelCor_1f:57:13 (00:12:f0:1f:57:13)
    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 0011 1110 .... = Sequence number: 2878
    Frame check sequence: 0x6ed851bb [unverified]
    [FCS Status: Unverified]
```

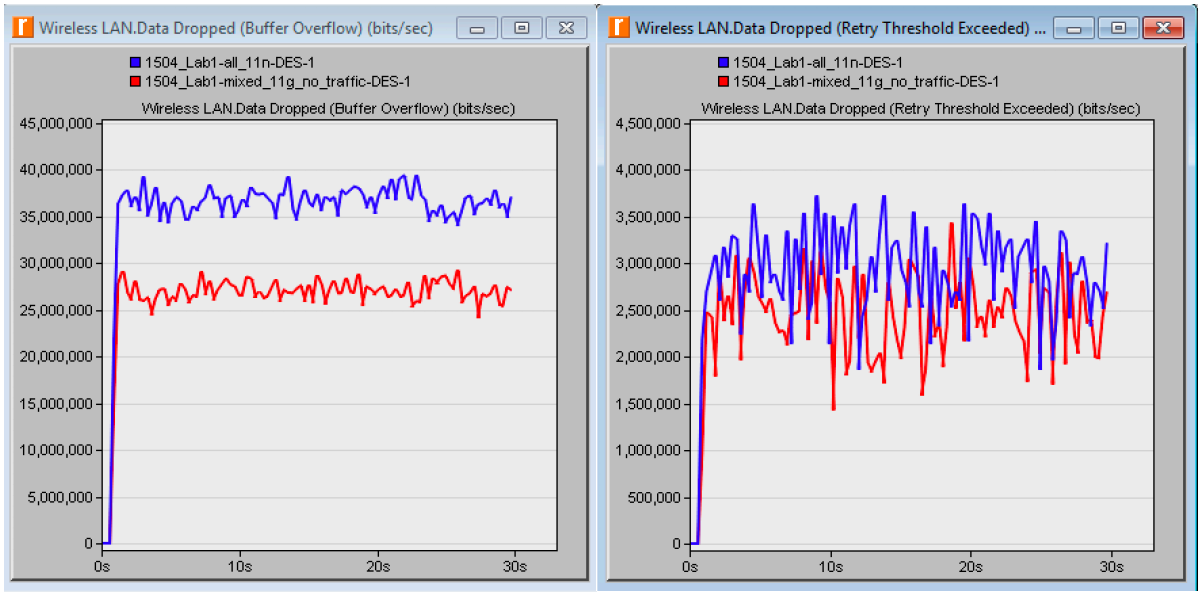
# Part 2. Planning Wireless LAN Network Deployments

### Mini Lab1: Mixed 11g/11n WLAN Performance

It is general notion that legacy STAs in the BSS will be detrimental to network performance. Here we see a situation where it actually improves the 11n throughput when CTS-to-self protection is enabled. The Data Dropped (Retry Threshold Exceeded) bps is almost the same in both scenarios the loss of packets due contention conditions is the same across both scenarios. However, in mixed_11g_no_traffic scenario, the higher layer packets are sent at a much faster rate which is inferred from lesser Data Dropped (Buffer Overflow) bps and lesser Media Access Delay (sec). In the presence of legacy 802.11g STAs and with CTS-to-self is enabled, a 11n STAs transmits a CTS at 11g data rate ahead of A-MSDU frames transmitted at 11n data rates to protect them from 11g devices. Recovery from small CTS frame collisions is much faster compared to recovery from huge A-MSDU frame collisions. Hence having legacy devices indirectly improves network throughput.

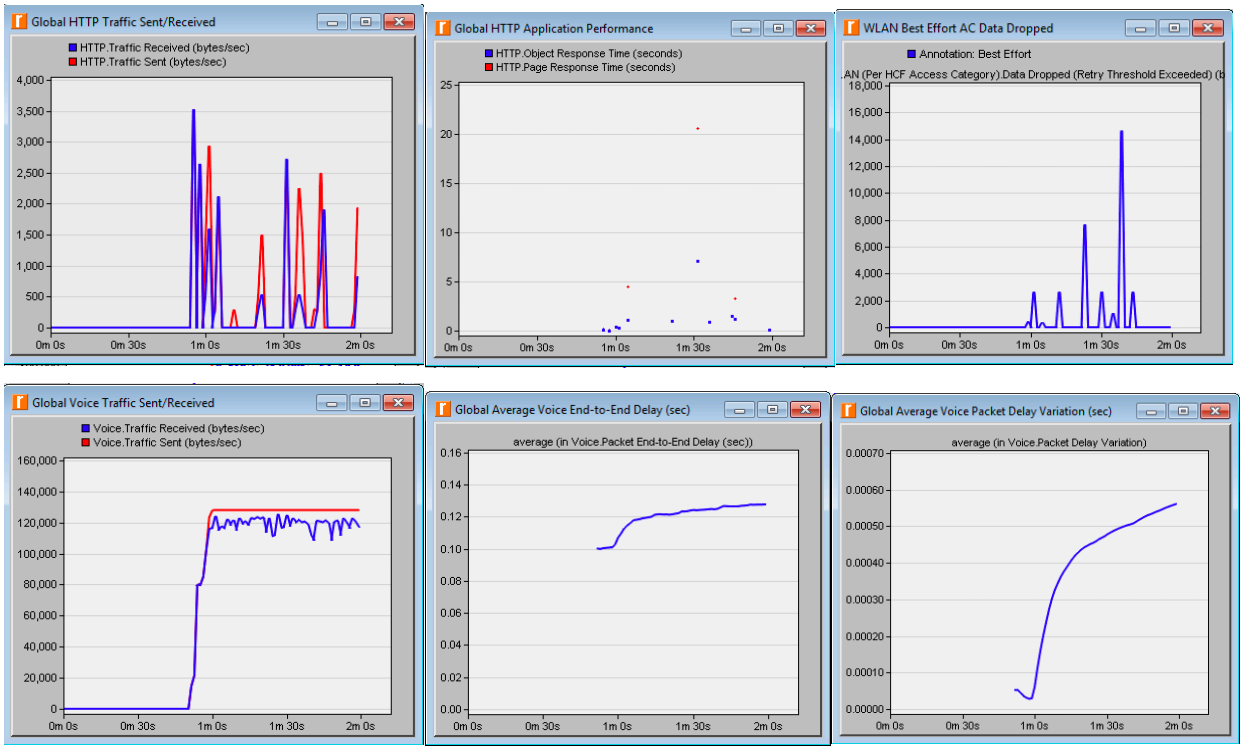


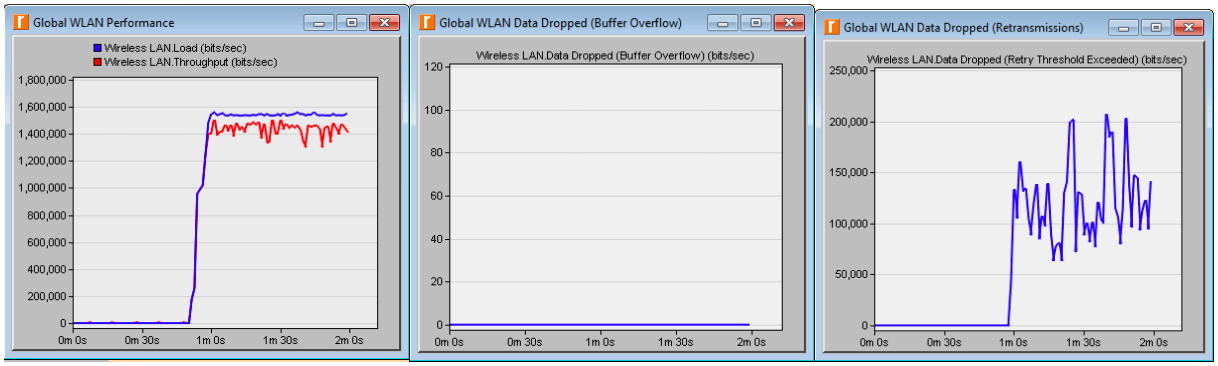






**Mini Lab2: Improving Performance with QoS Aware Wireless LAN Layer**

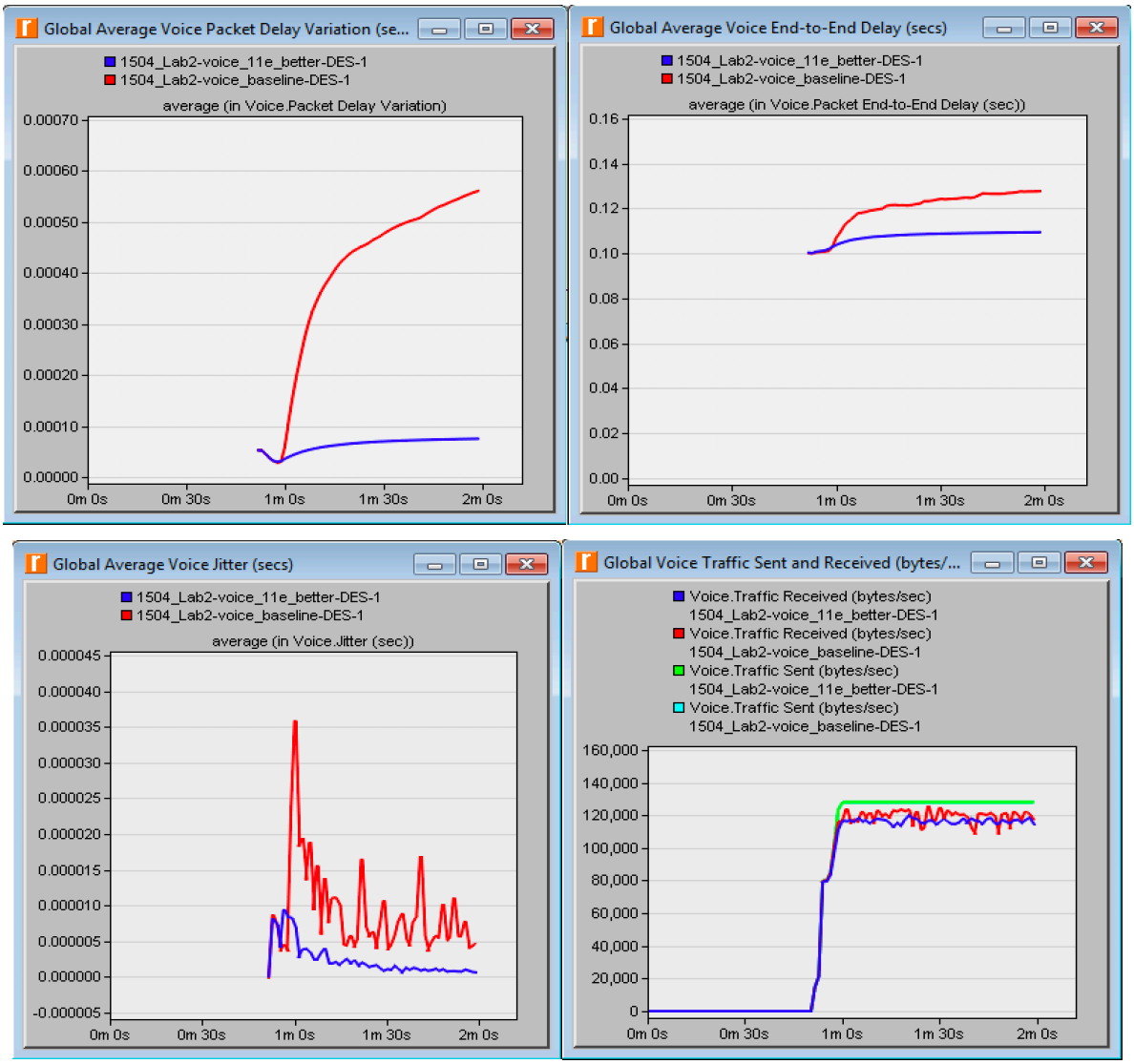
The following graph is the WLAN performance result under best-effort HTTP service for voice and http. In conclusion, with default 11e parameters it is observed that voice application has a better throughput than the HTTP. High number of WLAN layer retransmissions implies the main bottleneck at layer-2 needs to be tackled for further improvement.

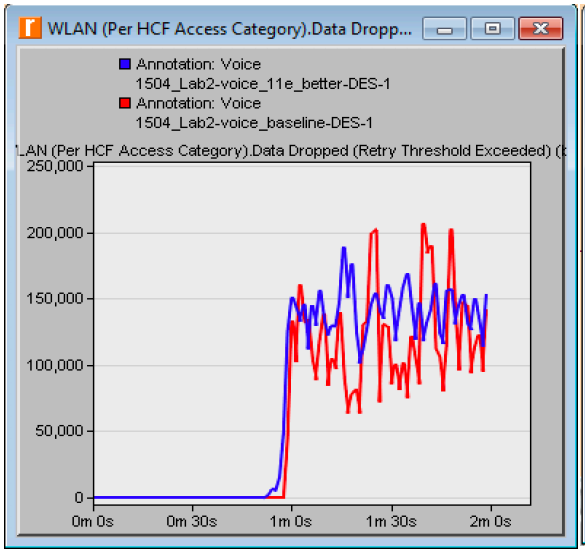


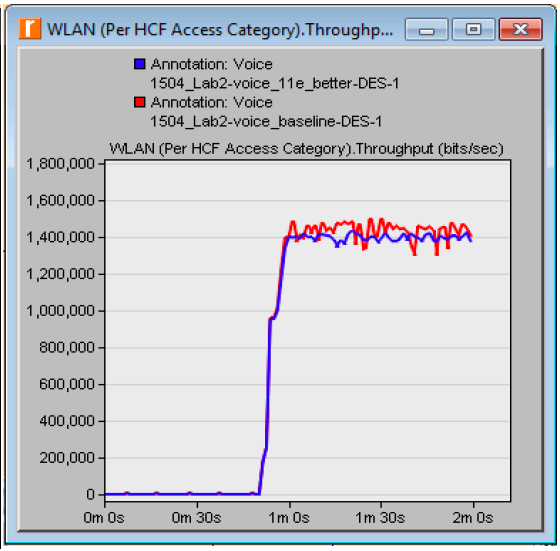


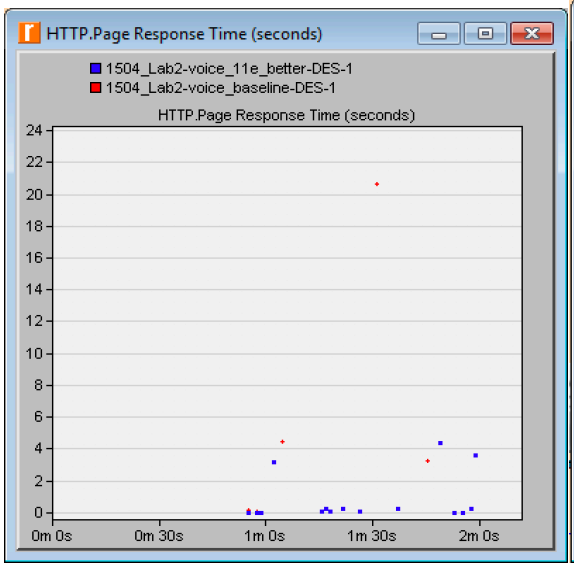

## Performance tuning for 11e network

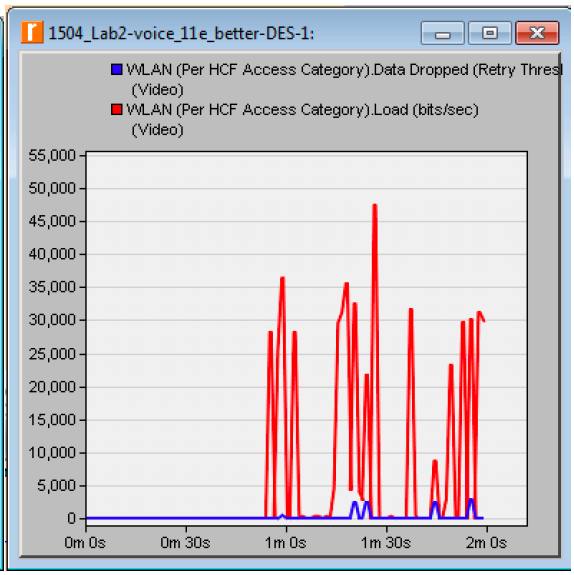
By adjusting related WLAN 802.11e parameters, the quality of voice calls across the network has been increased by reducing end-to-end, delay variation and jitter values as well as increasing the percentage of voice traffic that could be successfully delivered from source to destination.

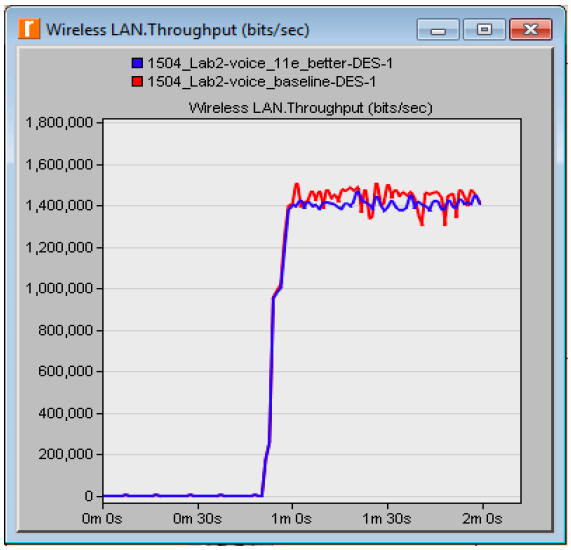



WLAN (Per HCF Access Category).Data Dropp...
Annotation: Voice
1504_Lab2-voice_11e_better-DES-1
Annotation: Voice
1504_Lab2-voice_baseline-DES-1
LAN (Per HCF Access Category).Data Dropped (Retry Threshold Exceeded) (
250,000
200,000
150,000
100,000
50,000
0
0m 0s
0m 30s
1m 0s
1m 30s
2m 0s


WLAN (Per HCF Access Category).Throughp...
Annotation: Voice
1504_Lab2-voice_11e_better-DES-1
Annotation: Voice
1504_Lab2-voice_baseline-DES-1
WLAN (Per HCF Access Category).Throughput (bits/sec)
1,800,000
1,600,000
1,400,000
1,200,000
1,000,000
800,000
600,000
400,000
200,000
0
0m 0s
0m 30s
1m 0s
1m 30s
2m 0s


HTTP.Page Response Time (seconds)
1504_Lab2-voice_11e_better-DES-1
1504_Lab2-voice_baseline-DES-1
HTTP.Page Response Time (seconds)
24
22
20
18
16
14
12
10
8
6
4
2
0
0m 0s
0m 30s
1m 0s
1m 30s
2m 0s


1504_Lab2-voice_11e_better-DES-1:
WLAN (Per HCF Access Category).Data Dropped (Retry Thres
(Video)
WLAN (Per HCF Access Category).Load (bits/sec)
(Video)
55,000
50,000
45,000
40,000
35,000
30,000
25,000
20,000
15,000
10,000
5,000
0
0m 0s
0m 30s
1m 0s
1m 30s
2m 0s


Wireless LAN.Throughput (bits/sec)
1504_Lab2-voice_11e_better-DES-1
1504_Lab2-voice_baseline-DES-1
Wireless LAN.Throughput (bits/sec)
1,800,000
1,600,000
1,400,000
1,200,000
1,000,000
800,000
600,000
400,000
200,000
0
0m 0s
0m 30s
1m 0s
1m 30s
2m 0s

**Conclusion**

From Lab 1, the wireless host sends frames to the first-hop-router through an access point with the MAC of itself to the MAC of first-hop-router and with the IP of itself to the IP of the destination, the reserved relationship applies when the other host is trying to connect with this wireless host. The wireless host would send an ASSOCIATION frame to associate with the access point at beginning, and when it is done with the association, it will send DISASSOCIATION frame to access point, then the connection is terminated, DHCP will release the IP from the wireless host.

From the mini Lab 1 of Lab2, when CTS-self-protection is enabled, the throughput of 11n network actually gets improved instead of expected to be lower at the beginning. It is general notion that legacy STAs in the BSS will be detrimental to network performance.

From the mini Lab 2 of Lab2, by adjusting the voice related network parameters of http service type (streaming video, etc.), the quality of the voice calls is obviously improved. The end-to-end delay has been reduced, the percentage of voice traffic has been increased. Therefore, the type of service that http chooses can have a large impact on network performance.