

Name: J Viswaksena

Roll.No: AM.EN.U4AIE21035

Lab Assignment 4

Topics Covered – 802.11 Protocol, Beacon Frame, Association and Disassociation

Q1. Identify the frequency of Beacon Frames for the two Aps.

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

Answer:-

Source: Cisco-Li_f7:1d:51 Destination: Broadcast Beacon frame, BI=100, **SSID="30 Munroe St"**

Source: LinksysG_67:22:94 Destination: 7f:26:ff:ff:ff:ff Beacon frame, BI=100, **SSID="linksys12"**[Malformed Packet: length of contained item exceeds length of containing item]

Q2. What are the intervals of time between the transmissions of the beacon frames from the linksys_ses_24086 access point? From the 30 Munroe St. access point?

Answer:-

30 Munroe St

```
[FCS Status: Unverified]
  IEEE 802.11 Wireless Management
    Fixed parameters (12 bytes)
      Timestamp: 174319412160
      Beacon Interval: 0.102400 [Seconds]
      > Capabilities Information: 0x0601
    Tagged parameters (119 bytes)
      Tag: SSID parameter set: "30 Munroe St"
        Tag Number: SSID parameter set (0)
        Tag length: 12
        SSID: "30 Munroe St"
      Tag: Supported Rates 1(B), 2(B), 5.5(B), 11(B), [Mbit/sec]
```

Timestamp: 174319412160

```

1011 0010 1100 .... = Sequence number: 2860
Frame check sequence: 0x4c2dfbc0 [unverified]
[FCS Status: Unverified]
√ IEEE 802.11 Wireless Management
  √ Fixed parameters (12 bytes)
    Timestamp: 174319616391
    Beacon Interval: 0.102400 [Seconds]
  > Capabilities Information: 0x0601
  √ Tagged parameters (119 bytes)
    √ Tag: SSID parameter set: "30 Munroe St"
      Tag Number: SSID parameter set (0)
      Tag length: 12
      SSID: "30 Munroe St"

```

Timestamp: 174319616391

Time interval: 174319616391 – 174319412160 = 204231 microseconds

linksys12

```

1100 0000 0011 .... = Sequence number: 3075
Frame check sequence: 0x6d393521 [unverified]
[FCS Status: Unverified]
√ IEEE 802.11 Wireless Management
  √ Fixed parameters (12 bytes)
    Timestamp: 9534922036096
    Beacon Interval: 0.102400 [Seconds]
  > Capabilities Information: 0x0011
  √ Tagged parameters (26 bytes)
    √ Tag: SSID parameter set: "linksys12"
      Tag Number: SSID parameter set (0)
      Tag length: 9
      SSID: "linksys12"

```

Timestamp: 9534922036096

```

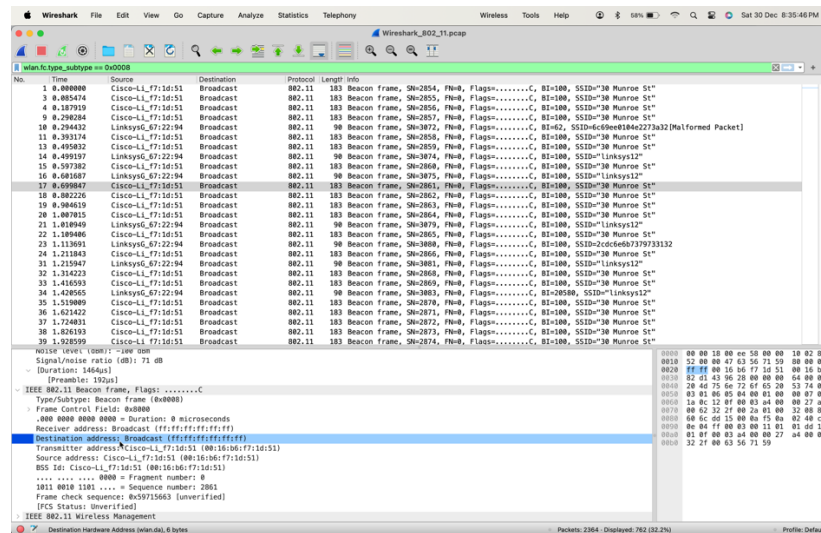
1100 0000 0111 .... = Sequence number: 3079
Frame check sequence: 0x324da246 [unverified]
[FCS Status: Unverified]
√ IEEE 802.11 Wireless Management
  √ Fixed parameters (12 bytes)
    Timestamp: 9534922445240
    Beacon Interval: 0.102400 [Seconds]
  > Capabilities Information: 0x0408
  √ Tagged parameters (26 bytes)
    √ Tag: SSID parameter set: "linksys12"
      Tag Number: SSID parameter set (0)
      Tag length: 9
      SSID: "linksys12"

```

Timestamp: 9534922445240

Time interval: 9534922445240 – 9534922036096 = 409144

Q3. What is the destination Address for Beacon Frames?



No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	Cisco-L1_f7:1d:51	Broadcast	802.11	183	Beacon Frame, Src=2854, Prio=0, Flags=.....C, B1=100, SSID=38 Munroe St"
3	0.085474	Cisco-L1_f7:1d:51	Broadcast	802.11	183	Beacon Frame, Src=2855, Prio=0, Flags=.....C, B1=100, SSID=38 Munroe St"
4	0.187919	Cisco-L1_f7:1d:51	Broadcast	802.11	183	Beacon Frame, Src=2859, Prio=0, Flags=.....C, B1=100, SSID=38 Munroe St"
9	0.296384	Cisco-L1_f7:1d:51	Broadcast	802.11	183	Beacon Frame, Src=2857, Prio=0, Flags=.....C, B1=100, SSID=38 Munroe St"
10	0.294332	LinksysG_67:22:94	Broadcast	802.11	90	Beacon Frame, Src=3872, Prio=0, Flags=.....C, B1=42, SSID=6c9ee8184e2773a32 [Malformed Packet]
11	0.393174	Cisco-L1_f7:1d:51	Broadcast	802.11	183	Beacon Frame, Src=2858, Prio=0, Flags=.....C, B1=100, SSID=38 Munroe St"
13	0.495832	Cisco-L1_f7:1d:51	Broadcast	802.11	183	Beacon Frame, Src=2859, Prio=0, Flags=.....C, B1=100, SSID=38 Munroe St"
14	0.499197	LinksysG_67:22:94	Broadcast	802.11	90	Beacon Frame, Src=3874, Prio=0, Flags=.....C, B1=100, SSID=Linksys12"
15	0.597382	Cisco-L1_f7:1d:51	Broadcast	802.11	183	Beacon Frame, Src=2860, Prio=0, Flags=.....C, B1=100, SSID=38 Munroe St"
16	0.691887	LinksysG_67:22:94	Broadcast	802.11	90	Beacon Frame, Src=3875, Prio=0, Flags=.....C, B1=100, SSID=Linksys12"
17	0.699447	Cisco-L1_f7:1d:51	Broadcast	802.11	183	Beacon Frame, Src=2861, Prio=0, Flags=.....C, B1=100, SSID=38 Munroe St"
18	0.882226	Cisco-L1_f7:1d:51	Broadcast	802.11	183	Beacon Frame, Src=2862, Prio=0, Flags=.....C, B1=100, SSID=38 Munroe St"
19	0.984619	Cisco-L1_f7:1d:51	Broadcast	802.11	183	Beacon Frame, Src=2863, Prio=0, Flags=.....C, B1=100, SSID=38 Munroe St"
20	1.007915	Cisco-L1_f7:1d:51	Broadcast	802.11	183	Beacon Frame, Src=2864, Prio=0, Flags=.....C, B1=100, SSID=38 Munroe St"
21	1.018949	LinksysG_67:22:94	Broadcast	802.11	90	Beacon Frame, Src=3879, Prio=0, Flags=.....C, B1=100, SSID=Linksys12"
22	1.109486	Cisco-L1_f7:1d:51	Broadcast	802.11	183	Beacon Frame, Src=2865, Prio=0, Flags=.....C, B1=100, SSID=38 Munroe St"
23	1.113991	LinksysG_67:22:94	Broadcast	802.11	90	Beacon Frame, Src=3880, Prio=0, Flags=.....C, B1=100, SSID=2c0c6e6b739733132
24	1.211843	Cisco-L1_f7:1d:51	Broadcast	802.11	183	Beacon Frame, Src=2866, Prio=0, Flags=.....C, B1=100, SSID=38 Munroe St"
31	1.215847	LinksysG_67:22:94	Broadcast	802.11	90	Beacon Frame, Src=3881, Prio=0, Flags=.....C, B1=100, SSID=Linksys12"
32	1.314223	Cisco-L1_f7:1d:51	Broadcast	802.11	183	Beacon Frame, Src=2868, Prio=0, Flags=.....C, B1=100, SSID=38 Munroe St"
33	1.416593	Cisco-L1_f7:1d:51	Broadcast	802.11	183	Beacon Frame, Src=2869, Prio=0, Flags=.....C, B1=100, SSID=38 Munroe St"
34	1.420555	LinksysG_67:22:94	Broadcast	802.11	90	Beacon Frame, Src=3883, Prio=0, Flags=.....C, B1=100, SSID=Linksys12"
35	1.519889	Cisco-L1_f7:1d:51	Broadcast	802.11	183	Beacon Frame, Src=2870, Prio=0, Flags=.....C, B1=100, SSID=38 Munroe St"
36	1.621422	Cisco-L1_f7:1d:51	Broadcast	802.11	183	Beacon Frame, Src=2871, Prio=0, Flags=.....C, B1=100, SSID=38 Munroe St"
37	1.724931	Cisco-L1_f7:1d:51	Broadcast	802.11	183	Beacon Frame, Src=2872, Prio=0, Flags=.....C, B1=100, SSID=38 Munroe St"
38	1.826193	Cisco-L1_f7:1d:51	Broadcast	802.11	183	Beacon Frame, Src=2873, Prio=0, Flags=.....C, B1=100, SSID=38 Munroe St"
39	1.928599	Cisco-L1_f7:1d:51	Broadcast	802.11	183	Beacon Frame, Src=2874, Prio=0, Flags=.....C, B1=100, SSID=38 Munroe St"

Wireshark details pane for frame 18:

- IEEE 802.11 Beacon Frame, Flags:C
- Type/Subtype: Beacon Frame (80000)
- Frame Control Field: 80000
- Duration: 0 microseconds
- Receiver address: Broadcast (ff:ff:ff:ff:ff:ff)
- Transmitter address: Cisco-L1_f7:1d:51 (00:16:b6:f7:1d:51)
- Source address: Cisco-L1_f7:1d:51 (00:16:b6:f7:1d:51)
- BSS Id: Cisco-L1_f7:1d:51 (00:16:b6:f7:1d:51)
- Sequence number: 2861
- Frame check sequence: 8c59715663 [unverified]
- [FCS Status] Unverified

Packets: 2364 - Displayed: 762 (32.2%)

Q4. What are the three MAC Addresses used in an Association Request?

Solution:

Destination address, Transmitter address and BSS Id are the three MAC Addresses

From the previous screenshot:

Destination address: ff:ff:ff:ff:ff:ff

Transmitter address: 00:16:b6:f7:1d:51

BSS Id: 00:16:b6:f7:1d:51

Q5. For the Second AP to which the device tries to associate, is it Active or Passive scanning?

Solution:

Based on the destination address: ff:ff:ff:ff:ff:ff => **Passive scanning**, if to a specific address => **Active scanning**.

30 Munroe St: Passive scanning

Wireshark_802.11.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

wlan.fc.type_subtype == 0x04

No.	Time	Source	Destination	Protocol	Length	Info
50	2.297613	IntelCor_1f:57:13	Broadcast	802.11	79	Probe Request, SN=576, FN=0, Flags=.....C, SSID="Home WIFI"
87	4.298449	IntelCor_1f:57:13	Broadcast	802.11	78	Probe Request, SN=598, FN=0, Flags=.....C, SSID="phoiphas"
117	6.299705	IntelCor_1f:57:13	Broadcast	802.11	79	Probe Request, SN=620, FN=0, Flags=.....C, SSID="concourse"
118	6.300439	IntelCor_1f:57:13	Broadcast	802.11	70	Probe Request, SN=621, FN=0, Flags=.....C, SSID="wildcard (Bro
171	8.299988	IntelCor_1f:57:13	Broadcast	802.11	77	Probe Request, SN=642, FN=0, Flags=.....C, SSID="linksys"
214	10.300585	IntelCor_1f:57:13	Broadcast	802.11	75	Probe Request, SN=664, FN=0, Flags=.....C, SSID="hfmpc"
260	12.300694	IntelCor_1f:57:13	Broadcast	802.11	75	Probe Request, SN=686, FN=0, Flags=.....C, SSID="BOHO2"
297	14.301102	IntelCor_1f:57:13	Broadcast	802.11	77	Probe Request, SN=708, FN=0, Flags=.....C, SSID="BOwDOIN"
1592	46.581961	IntelCor_1f:57:13	Broadcast	802.11	70	Probe Request, SN=730, FN=0, Flags=.....C, SSID="wildcard (Bro
1594	46.586825	IntelCor_d1:b6:4f	Broadcast	802.11	94	Probe Request, SN=1575, FN=0, Flags=.....C, SSID="30 Munroe St
1595	46.587567	IntelCor_d1:b6:4f	Broadcast	802.11	82	Probe Request, SN=1575, FN=0, Flags=.....C, SSID="wildcard (Bro
1629	46.780197	IntelCor_d1:b6:4f	Broadcast	802.11	82	Probe Request, SN=1577, FN=0, Flags=.....C, SSID="wildcard (Bro
1737	49.614478	IntelCor_d1:b6:4f	Broadcast	802.11	99	Probe Request, SN=1606, FN=0, Flags=.....C, SSID="linksys_SES
1820	53.761198	IntelCor_d1:b6:4f	Broadcast	802.11	99	Probe Request, SN=1612, FN=0, Flaes=.....C, SSID="linksys SES

....00 = DS status: Not leaving DS or network is operating in AD-H
0.. = More Fragments: This is the last fragment
0... = 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.... = +HTC/Order flag: Not strictly ordered
 .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_d1:b6:4f (00:13:02:d1:b6:4f)
 Source address: IntelCor_d1:b6:4f (00:13:02:d1:b6:4f)
 BSS Id: Broadcast (ff:ff:ff:ff:ff:ff)

0000 00 00 18 00 ee 58 00 00 10 02 85 09 a0 00 e6 9cX.....
 0010 64 00 00 4a 48 88 49 e5 40 00 00 00 ff ff ff ffJH-I-@.....
 0020 ff ff 00 13 02 d1 b6 4f ff ff ff ff ff ff 70 62pb
 0030 00 0c 33 30 20 4d 75 6e 72 6f 65 20 53 74 01 0830 Munroe St
 0040 02 04 0b 16 0c 12 18 24 0a 01 07 32 04 30 48 60\$2 OH
 0050 6c dd 07 00 03 47 01 02 01 01 48 88 49 e5G.....H-I

11°C Mostly clear

Linksys: Passive scanning

Wireshark_802.11.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

wlan.fc.type_subtype == 0x04

No.	Time	Source	Destination	Protocol	Length	Info
50	2.297613	IntelCor_1f:57:13	Broadcast	802.11	79	Probe Request, SN=576, FN=0, Flags=.....C, SSID="Home WIFI"
87	4.298449	IntelCor_1f:57:13	Broadcast	802.11	78	Probe Request, SN=598, FN=0, Flags=.....C, SSID="phoiphas"
117	6.299705	IntelCor_1f:57:13	Broadcast	802.11	79	Probe Request, SN=620, FN=0, Flags=.....C, SSID="concourse"
118	6.300439	IntelCor_1f:57:13	Broadcast	802.11	70	Probe Request, SN=621, FN=0, Flags=.....C, SSID="wildcard (Bro
171	8.299988	IntelCor_1f:57:13	Broadcast	802.11	77	Probe Request, SN=642, FN=0, Flags=.....C, SSID="linksys"
214	10.300585	IntelCor_1f:57:13	Broadcast	802.11	75	Probe Request, SN=664, FN=0, Flags=.....C, SSID="hfmpc"
260	12.300694	IntelCor_1f:57:13	Broadcast	802.11	75	Probe Request, SN=686, FN=0, Flags=.....C, SSID="BOHO2"
297	14.301102	IntelCor_1f:57:13	Broadcast	802.11	77	Probe Request, SN=708, FN=0, Flags=.....C, SSID="BOwDOIN"
1592	46.581961	IntelCor_1f:57:13	Broadcast	802.11	70	Probe Request, SN=730, FN=0, Flags=.....C, SSID="wildcard (Bro
1594	46.586825	IntelCor_d1:b6:4f	Broadcast	802.11	94	Probe Request, SN=1575, FN=0, Flags=.....C, SSID="30 Munroe St
1595	46.587567	IntelCor_d1:b6:4f	Broadcast	802.11	82	Probe Request, SN=1575, FN=0, Flags=.....C, SSID="wildcard (Bro
1629	46.780197	IntelCor_d1:b6:4f	Broadcast	802.11	82	Probe Request, SN=1577, FN=0, Flags=.....C, SSID="wildcard (Bro
1737	49.614478	IntelCor_d1:b6:4f	Broadcast	802.11	99	Probe Request, SN=1606, FN=0, Flags=.....C, SSID="linksys_SES
1820	53.761198	IntelCor_d1:b6:4f	Broadcast	802.11	99	Probe Request, SN=1612, FN=0, Flaes=.....C, SSID="linksys SES

....00 = DS status: Not leaving DS or network is operating in AD-H
0.. = More Fragments: This is the last fragment
0... = 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.... = +HTC/Order flag: Not strictly ordered
 .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 00 00 18 00 ee 58 00 00 10 02 85 09 a0 00 aa 9cX.....
 0010 0b 00 00 0e e5 cb 7b bc 40 00 00 00 ff ff ff ff-@.....
 0020 ff ff 00 12 f0 1f 57 13 ff ff ff ff ff ff 20 28 (.....
 0030 00 07 6c 69 6e 6b 73 79 73 01 08 82 84 0b 16 0clinksys s.....
 0040 12 18 24 32 04 30 48 60 6c e5 cb 7b bc2 OH' 1-{-

11°C Mostly clear