Foundation of Computer Networks - Wireshark Project Bhavin Oza (bo2115)

```
■ Apply a display filter ... <第/>
           Time Source
1 22:05:07.072457 Cisco-Li_f7:1d:51
2 22:05:07.134558 8c:cl:ae:c0:ea:2c
3 22:05:07.157931 Cisco-Li_f7:1d:51
4 22:05:07.260376 Cisco-Li_f7:1d:51
5 22:05:07.260357 IntelCor_d1:b6:4f
                                                                                            | Destination
| Broadcast
                                                                                                                              |Protocol | Length | Info
802.11 183 Beacon frame,
                                                                                                                                            Lengtlino
183 Beacon frame, SN=2854, FN=0, Flags=......C, BI=100, SSID=30 Munroe St
1624 PV1 Management[Malformed Packet]
183 Beacon frame, SN=2855, FN=0, Flags=.......C, BI=100, SSID=30 Munroe St
183 Beacon frame, SN=2856, FN=0, Flags=......C, BI=100, SSID=30 Munroe St
54 QoS Null function (No data), SN=1482, FN=0, Flags=......TC
                                                                                             8c:c1:ae:c0:ea:2c ...
Broadcast
Broadcast
Cisco-Li_f7:1d:51
                                                                                                                                             5 22:95:07.260557 Intellor_01:05:41
6 22:05:07.260558
7 22:05:07.261392 Intellor_01:06:4f
8 22:05:07.362741 Cisco-Li_f7:1d:51
10 22:05:07.366889 LinksysG_67:22:94
11 27:05:07.365811 Cisco-Li_f7:1d:51
                                                                                             IntelCor_d1:b6:4f ...
Cisco-Li_f7:1d:51
IntelCor_d1:b6:4f ...
                                                                                                                              802.11
802.11
802.11
802.11
                                                                                             Broadcast
  Broadcast
                                                                                                                               802.11
802.11
                                                                                                                                                                                                      Packets: 2364 - Displayed: 2364 (100.0%)
```

1). 30 Munroe St and linksys12

2). 1024 seconds

3). Source MAC: 00:16:b6:f7:1d:51

4). Destination MAC: ff:ff:ff:ff:ff

5). MAC BSSID Address: 00:16:b6:f7:1d:51

6). Support rates \rightarrow 1,2,5.5,11.0

```
    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 Number: Supported Rates (1)
    Tag length: 4
    Supported Rates: 1(B) (0x82)
    Supported Rates: 2(B) (0x84)
    Supported Rates: 5.5(B) (0x8b)
    Supported Rates: 11(B) (0x96)
```

Extended support rates \rightarrow 6.0,9.0, 12.0, 18.0, 24.0, 36.0, 48.0 and 54.0 mbps

Foundation of Computer Networks - Wireshark Project Bhavin Oza (bo2115)

```
    Tag: Extended Supported Rates 6(B), 9, 12(B), 18, 24(B), 36, 48, 54, [Mbit/sec]
    Tag Number: Extended Supported Rates (50)
    Tag length: 8
    Extended Supported Rates: 6(B) (0x8c)
    Extended Supported Rates: 9 (0x12)
    Extended Supported Rates: 12(B) (0x98)
    Extended Supported Rates: 18 (0x24)
    Extended Supported Rates: 24(B) (0xb0)
    Extended Supported Rates: 36 (0x48)
    Extended Supported Rates: 48 (0x60)
    Extended Supported Rates: 54 (0x6c)
```

7). MAC address for sender host: 00:13:02:d1:b6:4f

The MAC address for the destination, that is the first hop router to which the host is connected:

00:16:b6:f4:eb:a8

MAC address for the BSS: 00:16:b6:f7:1d:51 IP address of the sender host: 192.168.1.109

Destination address: 128.199.245.12

Destination MAC address of the frame containing the SYN, different from the destination IP address of the IP packet contained within this frame.

8). TCP SYNACK \rightarrow t = 24.827751 (received)

Sender's MAC address (with TCP SYNACK segment) \rightarrow 00:16:b6:f4:eb:a8 \rightarrow 1st Hop router.

Destination's MAC address → 91:2a:b0:49:b6:4f (host)

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

Server sending TCP SYNACK → 128.199.245.12

9). t = 49.583615, DHCP releases a message to the DHCP server in the network that the host is leaving.

t = 49.609617, host sends a DEAUTHENTICATION frame.

A DISASSOCIATION request is expected.

- 10). first AUTHENTICATION is at time t = 49.638857
- 11). host will request an association to be open using Open system authentication algorithm.
- 12). No
- 13). At t = 63.168087, AUTHENTICATION frame sent from 00:13:02:d1:b6:4f to 00:16:b7:f7:1d:51

At t = 63.169071, AUTHENTICATION sent in the reverse direction from BSS to the wireless host.

14). At t = 63.169910, AUTHENTICATION REQUEST frame sent from 00:13:02:d1:b6:4f to 00:16:b7:f7:1d:51

At t = 63.192101, ASSOCIATE RESPONSE sent in the reverse direction from BSS to wireless host.

Foundation of Computer Networks - Wireshark Project Bhavin Oza (bo2115)

15). For ASSOCIATION REQUEST frames, the supported rates advertised are 1, 2, 5.5, 11, 6, 9, 12, 18, 24, 32, 48 and 54 Mbps.

The rates in ASSOCIATE RESPONSE would be the same.

16). At t = 2.297613, PROBE REQUEST is sent from 00:12:f0:1f:57:13 to ff:ff:ff:ff:ff:ff and BSSID of ff:ff:ff:ff:ff.

At t = 2.300697, PROBE RESPONSE is sent from 00:16:b6:f7:1d:51, destination and BSSID of 00:16:b6:f7:1d:51

In active scanning, a PROBE REQUEST request is used by a host to find an access point. A PROBE RESPONSE response is sent by the access point to the host.