

Wifi Beacons

We have a data file with captured wifi frames. Using that file, analyze the file and answer the following questions

- Find the beacon frame for the wireless network. What's the SSID? Include a screenshot showing you found the SSID

11 0.000552	Cisco-Li_a1:7f:65	Broadcast	802.11	90 Beacon frame, SN=117, FN=0, Flags=....., BI=1...
12 0.001536	ArubaNet_e8:f0:e0 (.. IntelCor_ba:85:ba (..	802.11	16 Request-to-send, Flags=.....	
13 0.001532	ArubaNet_e8:f0:e0 (..	802.11	10 Clear-to-send, Flags=.....	
14 0.001532	IntelCor_ba:85:ba (.. ArubaNet_e8:f0:e0 (..	802.11	28 802.11 Block Ack, Flags=.....	
15 0.008706	IntelCor_43:f5:94 (.. ArubaNet_e8:c7:20 (..	802.11	16 Power-Save poll, Flags=...P....	
16 0.009218	IntelCor_43:f5:94 (.. ArubaNet_e8:c7:20 (..	802.11	16 Power-Save poll, Flags=...P....	

> Frame 11: 90 bytes on wire (720 bits), 90 bytes captured (720 bits)
> IEEE 802.11 Beacon frame, Flags:
✓ IEEE 802.11 wireless LAN
✓ Fixed parameters (12 bytes)
Timestamp: 0x00000000772ef1e9
Beacon Interval: 0.102400 [Seconds]
> Capabilities Information: 0x0401
✓ Tagged parameters (54 bytes)
✓ Tag: SSID parameter set: Free_Candy
Tag Number: SSID parameter set (0)
Tag length: 10
SSID: Free_Candy

Free_Candy

- What is a Beacon interval? With wifi, what is the absolute minimum and maximum value for the beacon interval?

.102400 [seconds]

- What type of wireless network is broadcasting? Show a screenshot that shows how you found out.

802.11b

```

Tag length: 8
Supported Rates: 1(B) (0x82)
Supported Rates: 2(B) (0x84)
Supported Rates: 5.5(B) (0x8b)
Supported Rates: 11(B) (0x96)
Supported Rates: 18 (0x24)
Supported Rates: 24 (0x30)
Supported Rates: 36 (0x48)
Supported Rates: 54 (0x6c)
> Tag: DS Parameter set: Current Channel: 6
> Tag: Traffic Indication Map (TIM): DTIM 0 of 0 bitmap
> Tag: ERP Information
> Tag: ERP Information
✓ Tag: Extended Supported Rates 6, 9, 12, 48, [Mbit/sec]
  Tag Number: Extended Supported Rates (50)
  Tag length: 4
  Extended Supported Rates: 6 (0x0c)
  Extended Supported Rates: 9 (0x12)
  Extended Supported Rates: 12 (0x18)
  Extended Supported Rates: 48 (0x60)

```

- What encryption, if any, is the network using?
None
- With the beacon frame, the device is manufactured by Cisco (Linksys), but Cisco did not actually make the radio in the base station. Who did?
Broadcom
- Of the many values in this beacon frame, one of them isn't actually required by the access point. It could be blank/empty. Which one is it?
ERP
- The BTS in this beacon supports "short time slots". This setting is enabled. Find the setting (byte) in the beacon frame that indicates this and include a screenshot. What does this value indicate? What impact does it have on a network?

```
.... .1.. .... = Short Slot Time: In use
```

Short Slot Time indicates that the time between communications is reduced, increasing throughput. All clients must also be capable of keeping up with this pace.