BEACON FRAME

**INTRODUCTION**:

* A beacon frame is a type of management frame that is transmitted by an access point (AP) in a wireless local area network (WLAN).
* The primary purpose of a beacon frame is to announce the presence of an AP and to provide information about the WLAN, such as the network name (SSID (service set identifier)), security settings, and available data rates.

**WORKING OF BEACON:**

The working of a beacon frame in a WLAN can be described in the following steps:

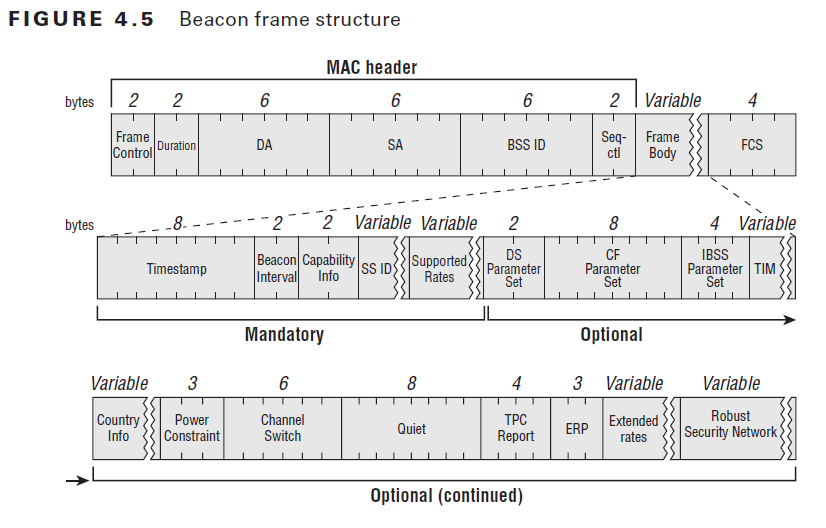
* **Beacon frame generation**: An access point (AP) generates a beacon frame periodically, typically every 100 milliseconds.
* Beacons are sent periodically at a time called **Target Beacon Transmission Time (TBTT).**
* 1 TU = 1024 microseconds.
* Beacon interval =100 TU (100x 1024 microseconds or 102.4 milliseconds).
* The beacon frame contains information about the WLAN, such as the network name (SSID), security settings, available data rates, and other parameters.
* **Beacon frame transmission**: Once generated, the AP broadcasts the beacon frame over the air using a predetermined channel and transmission power. The beacon frame is transmitted at a low data rate to ensure that it is received by all devices within range of the AP.
* **Device reception:** Devices within range of the AP receive the beacon frame and extract the information contained within it. Devices can use this information to determine if the WLAN is available, and if so, whether they should attempt to connect to it.
* **Network discovery:** If a device determines that the WLAN is available and it is configured to connect to the network, it can attempt to associate with the AP. This process involves sending a request to the AP to join the network, and if successful, the device can begin communicating with other devices on the network.
* **Signal quality monitoring:** Devices can also use the information in the beacon frame to monitor the quality of the wireless signal from the AP. This information can be used to determine the optimal connection to the AP, such as by selecting a different channel or adjusting the transmission power.

**IN AN IBSS NETWORK:**

* In an IBSS (INDEPENDENT BASIC SERVICE SET), stations use beacon frames for time synchronization and to maintain a common set of parameters for the IBSS.
* Because there is no central access point taking care of the beacon generation, the process is distributed.
* The first station to create the ad hoc network defines the **beacon interval**and announces it in the subsequent probe requests and responses.
* All stations joining the IBSS learn this interval. When the time comes for the next beacon, each station treats the beacon as the next packet to send.
* This means that each station of the IBSS does the following:

1. Interrupts its countdown for the next packet to send or wakes up if it was in Power Save mode.
2. Picks up a random number between zero and twice CWmin and 2× aSlotTime.
3. Counts down to zero from that number.
4. The first station to reach zero sends the beacon.
5. Hearing the beacon, the other stations remove the beacon from their network stack and resume their previous activity.

**BEACON FRAME FORMAT:**

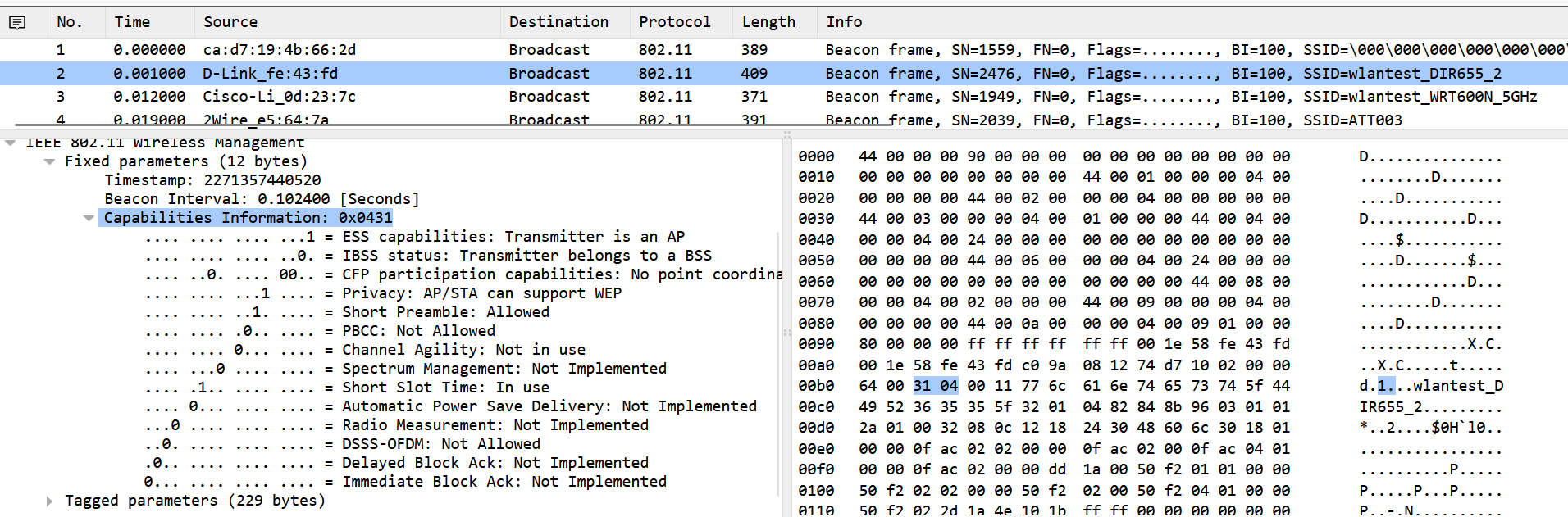
****

In the frame body section, there are few mandatory fields & few optional fields.  Here are the mandatory fields in a Beacon frame.  
1. Timestamp (8 byte)  
2. Beacon Interval (2 byte)  
3. Capability info (2 byte)  
4. SSID (variable size)  
5. Supported Rates (variable size)

**Timestamp (8 byte)**: A value representing the time on the access point, which is the number of microseconds the AP has been active. When timestamp reach its max (2^64 microsecond or ~580,000 years) it will reset to 0. This field contain in Beacon Frame & Probe Response frame.

**Beacon Interval (2 byte):** Beacon Interval field represent the number of time units (TU) between target beacon transmission times (TBTT). Default value is 100TU (102.4 milliseconds)

**Capability Information (2 byte)**: This field contains number of subfields that are used to indicate requested or advertised optional capabilities.

* + 

**SSID:** Present in all Beacons, probe requests, probe responses, association request & re-association requests. Element ID is 0 for the SSID IE. SSID could have maximum of 32 characters.

**Supported rates:** The supported rates field in the beacon frame provides critical information about the data rates that are supported by the AP or base station, allowing devices to connect to the network at the appropriate rate and enabling efficient communication on the WLAN.

* The supported rates field is an optional field in the beacon frame, but it is commonly included. It is a variable-length field that can contain up to **15 supported data rates**, with each rate specified in units of **500 kilobits per second (kbps).**
* The supported rates field can contain a mix of mandatory and optional rates. Mandatory rates are those that must be supported by all devices to connect to the network, while optional rates are those that are supported by some devices but not others.
* The specific rates included in the supported rates field can vary depending on the WLAN standard being used, such as IEEE (Institute for Electrical and Electronics Engineers) 802.11a, IEEE 802.11b, IEEE 802.11g, or IEEE 802.11n. In general, the supported rates field will include a mix of basic rates and additional rates, with basic rates being those that are required for initial connection and additional rates being those that provide higher throughput.

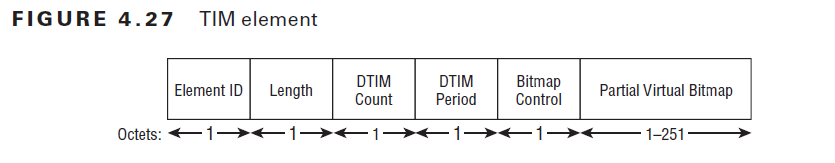
**FH (Frequency Hopping) parameter set**:  
Used by legacy Frequency Hopping (FH) stations

**DS Parameter (2 byte):**  
Present with beacon frame generated by stations using Clause 15, 18 or 19 PHY or if the beacon sent using one of the rates defined by one of the clauses.

**CF Parameter (8 byte):**  
Used with PCF, unused in real networks

**IBSS parameter (4 byte)**:  
Present only within beacon frames generated by stations in IBSS (or Ad-Hoc network).

**TRAFFIC INDICATION MAP(TIM)**: The TIM field in the beacon frame provides information about the presence of buffered frames at the AP, allowing devices to efficiently retrieve any pending frames and maintain smooth communication on the WLAN.



* The **TIM (Traffic Indication Map)** field in the beacon frame of a wireless local area network (WLAN) is used to indicate the presence of buffered unicast or multicast frames at the access point (AP). The TIM field is optional and may not be included in all beacon frames.
* When the TIM field is present, it indicates the availability of buffered frames at the AP that are waiting to be delivered to the intended recipient. The TIM field includes several subfields that provide information about the buffered frames, including the following:
* **DTIM Count**: This subfield indicates the number of beacon intervals that must elapse before the delivery traffic indication message (DTIM) is sent. The DTIM is a special beacon frame that is used to notify devices of the presence of multicast or broadcast traffic that is buffered at the AP.
* **DTIM Period:** This subfield indicates the number of beacon intervals between successive DTIM frames.
* **Bitmap Control:** This subfield indicates whether the bitmap subfield is present and the format of the bitmap.
* **Partial Virtual Bitmap:** This subfield contains a bitmap that indicates which stations have frames buffered at the AP. Each bit in the bitmap corresponds to a specific station, and a value of 1 indicates that frames are buffered for that station.
* **Virtual Bitmap:** This subfield contains a bitmap that indicates which stations have frames buffered at the AP. However, unlike the partial virtual bitmap, the virtual bitmap includes a bit for every station in the basic service set (BSS).

The TIM field is used by devices to determine if there are buffered frames waiting for them at the AP. If a device sees a TIM field in a beacon frame, it can request the buffered frames using the appropriate protocol, such as the Point Coordination Function (PCF) in the IEEE 802.11 standard.

**Country**:  
Each country has regulatory bodies that limit the channels or power levels allowed in their regulatory domain. It defines the country of operation along with the allowed channels & maximum transmit power. This is not a mandatory field in a beacon.

* 12-13. FH Parameters & FH Pattern table (used by Legacy FH stations)

**Power Constraint (3 byte)**:  
This element is related to 802.11h. This is for UNII2 & UNII-2 extended (CH52,56,60,64 & CH100-139) where spectrum is used for other purposes like civilian airport radar, weather radar. So, to avoid interference with those systems AP should operate max power specified by these constraint fields.

**Channel Switch (6 byte)**:  
This is also related to 802.11h. When a radar blast is detected, all stations must leave the affected channel. The AP can set to announce to the cell which is the next channel.

**Quite (8 byte):**  
Another element related to 802.11h where an AP can request a quiet time during which no station should transmit to test the channel for the presence of radars.

**IBSS DFS (Dynamic Frequency Selection)** – used with 802.11h in IBSS

**TPC Report (4 byte)**:  
This element is also related to 802.11h. TPC Report element contain Transmit Power & Link Margin information, usually sent in response to a TPC Request element. Below shows the “TPC Report” element of a beacon frame.

**ERP Information (3 byte**):  
ERP element is present only on 2.4GHz network supporting 802.11g & it is present in beacon & probe responses. The non-ERP Present bit set to 1 in following conditions  
a. A nonERP station (legacy 802.11 or 802.11b) associate to the cell  
b. A neighbouring cell is detected, allowing only nonERP data rates  
c. Any other management frame (except probe request) is received from neighbouring cell supporting only nonERP data rates.

**Extended Supported Rates**: Extended Support Rates element specifies the supported rates not carried in the Supported Rates Element. It is only required if there are more than 8 supported rates.

**RSN– Robust Secure Network**:  
RSN information element used to indicate Authentication Cipher, Encryption Cipher & other RSN capability of stations. In the below RSN IE, it shows AP support 802.1X & 802.11r FT as Authentication Suites. Also, it uses AES (Advanced Encryption Standard) as pairwise cipher (for unicast traffic) & group cipher (for broadcast/multicast).