Legacy power save mode

* 1.what is the legacy
* 2. what is the power save
* 4.Ps-poll and non-Ps-poll
* 5.TIM (Traffic indication map)
* 6.DTIM (Delivery traffic indication map)

**legacy:**

Because it’s an old and initial power save mechanism.

1. 802.11 Wi-Fi standard
2. 802.11b
3. 802.11g
4. 802.11a

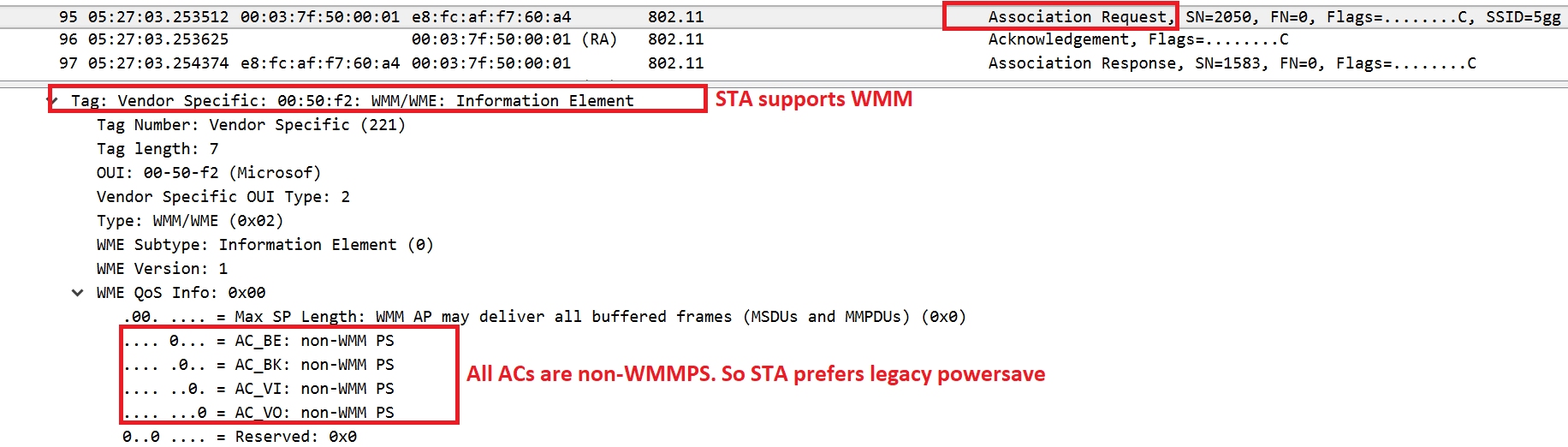
**What is the power save:**

1. Battery Saver, Power Saving, or Power Saving Mode is a feature available on all Android devices that aims to limit power consumption
2. so that your battery lasts a little longer until you get to charge it again.

**Note:** power save is a station and client feature.

**How to check device support legacy power save from sniffer capture**

* association request in this case you can see all access categories as 0(zero)
* AC\_ Vo=0
* AC\_VI=0
* AC\_BE=0
* AC\_BK=0



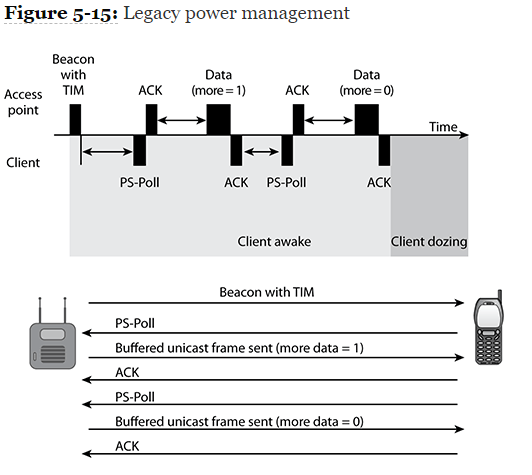
**Steps for Ps- Poll**

1. One client is connected to ap.
2. Client supports PS-poll mechanism from legacy power save.
3. After association response client sends one null data packet with power management bit 1 to ap.

Diagram

Description automatically generated

1. Ap replies with ack This indicates that client is going to sleep and ap agrees on the same. This time onwards ap started buffering any data that are intended for the sleeping client
2. When ap has buffer data, it indicates in beacon frame.
3. In beacon frame has Tim field under Tim there is partial virtual bitmap to indicate for which AID ap has buffer data.
4. The client generally wakes up at listen interval time.
5. Then Station checks the beacon and if the beacon has AID of this Station, then station knows that AP has buffer data.
6. Then station sends PS-poll frame to ap
7. AP sends ACK for PS -poll.
8. station is ready to receive buffer data.
9. AP started sending buffer data to station.
10. Now let’s assume AP has 2 buffer data packets for station. Upon receiving one PS-poll from station side, then AP send one data to station and gets the ack.
11. Inside the data, more data bit is 1 so station understood that AP has more buffer data, then station sends one more PS-poll frame to get data2
12. 13. whenever ap sends more data ==0 that time station will be understood there is no buffer data so it will send only ack to AP.



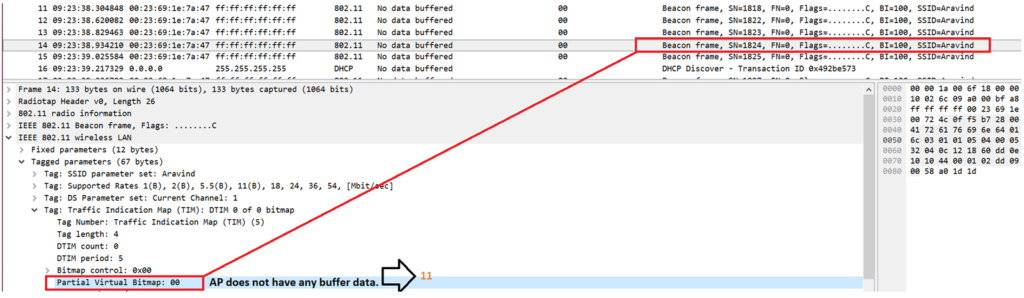
**Note**: here station does not send any null data with PM==1 to indicate its going for sleep again why?

1. If we see inside of PS-poll frame, there PM bit always 1.
2. so station does not have to send any extra frame to indicate ap about going to sleep.
3. in another way we think is station is already in power save but wake up to get the buffer data.
4. 14. AP removes buffer data indication from beacon for clients AID. This indicates AP does not have any buffer data

**Sniffer check for PS-poll sequence:**

Let’s see previous points inside Wireshark capture. Refer screenshot point to match with previous points for better understanding. Text, letter

Description automatically generated

15.we should see partial virtual bit map as 0x00 inside beacon so showing another beacon to indicate how it looks like 

**What is the PS- poll frame :**

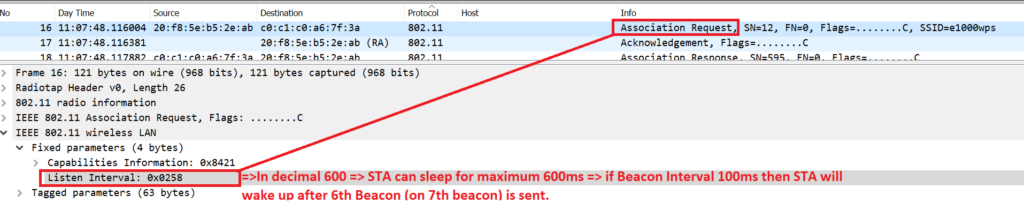
1. PS-poll frame is a special control frame as it doesn’t have duration field.
2. Instead it has AID and pm bit is always 1.

**One quick question:**

1. **if** there is no duration then how long other station will defer the medium after listening to PS-poll frame?
2. There is one fixed time: whoever listen PS-poll frame, they defer SIFS+ACK time.

**How long client can go for power save :**

In general station can go for power save for maximum listen interval time(ms) mention in association request frame.



For suppose listen interval 0x0248-in decimal 600==station can sleep for maximum 600ms== if beacon interval 100ms then station will wake up after 6th beacon (on 7th beacon) is sent.

**Note :**

1. but note that station says it will remain sleep for 600ms (above example), this does not mean station cannot wake up before 600ms.
2. Station can wake any time as per implementation but waking up at 7th beacon is expected by AP.

**How long AP can buffer data if client does not take buffer if client does not take buffer data on time?**

1. As we have observed station will wake up and get buffer data in best scenario.
2. But what if station does not get buffer data and AP will keep on indicating through beacon. there has to be some end to this right?
3. So inside ap per AID there is one timer call ending timer, if the ending timer time outs then ap drops all buffer packet for that station reset the timer.
4. There is no standard value for this ending timer.

**Non PS-poll**: 1.as station supports non- PS poll, after association done station sends one null frame to access point with PM=0 it means, station in awake state. Text, letter

Description automatically generated

Now ap sends all buffer data one by one without expecting any frame like PS-poll from station.

3.if more data bit set to 1 station should be in awake state. Once more data bit set to 0, then station sends null frame mode to ap indicting that statin is going to power save mode.in case of PS-poll no extra frame was sent to indicate ap that is goes for power save.

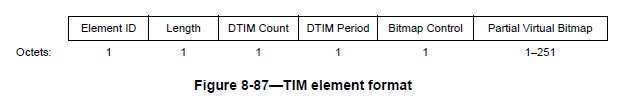
ap removes AID from PVB in beacon.

**How do we test PS-Poll or non-PS-Poll power save?**

1. In generally DHCP packet exchanges will use power save mechanism from ap side like
2. before ap sending DHCP offer ap will indicate in beacon for power save station and supports PS-poll or non-PS-Poll
3. We can start ping or iperf data from ap backend station wireless IP and see power save mechanism in sniffer capture.
4. Basically, any data from AP should use power save mechanism before sending to sleep stations.

**TIM (Traffic indication map):**

1. Traffic Indication Map (TIM) is an Information element and is part of the Beacon frame that is sent out by the Access Point at regular intervals.
2. The TIM Information element provides information on the current DTIM count and DTIM period and provides information on whether Buffered Multicast/Broadcast Data or unicast data for different 802.11 Stations are buffered at the Access Point.
3. The TIM information element is provided below for reference



The Element ID is 5.

**The Length** parameter indicates the length of the Information element starting from the DTIM Count to the end of the Partial Virtual Bitmap Octets.

**DTIM Count** –

1. is a down counter indicating the count till a DTIM Beacon is to be transmitted. When the DTIM count is zero, the beacon is a DTIM beacon and the Access Point will transmit buffered multicast/broadcast packets immediately after the DTIM beacon.

**DTIM Period** –

The DTIM Period indicates the number of successive beacons before a DTIM beacon transmission.

**Bitmap Control** –

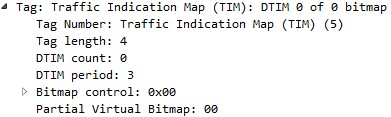
1. Bit 0 of the Bitmap control indicates whether there is buffered Multicast/Broadcast Data to be transmitted at the Access Point.
2. Bits 1-7 provide the Bitmap offset for the Partial Virtual Bitmap.

**Partial Virtual Bitmap** –

1. this is a bitmap of 1-251 octets (2008 bits) where-in each bit corresponds to an Association ID of a connected station.
2. It is termed as Partial virtual bitmap because only a section of the bitmap (the AIDs that have buffered unicast data at the AP) is transmitted in a beacon.

**NOTE:** The Access Point provides a Unique Identifier to a WLAN station on a successful association – that is termed as Association Identifier (AID) for the associated WLAN Station.

**The TIM information element wireless capture is shown below**



Text

Description automatically generated

Delivery Traffic Indication Map (DTIM):

1. After reviewing what the 802.11 standard says about DTIM. Let’s discuss in real world terms what a DTIM is and how it works.
2. You will specifically find DTIM in a management frame called a beacon under the TIM information element. DTIM is to broadcast / multicast traffic as TIM is to unicast traffic.
3. Under the TIM you will see DTIM count and DTIM period.

**Example:** DTIM COUNT / DTIM PERIOD

**DTIM Count** –

1. This field indicates how many beacon frames till the next DTIM.
2. A DTIM count field of 0 indicates that TIM is a DTIM.
3. A DTIM count field of 1 indicates the next beacon is a DTIM.

**DTIM Period** –

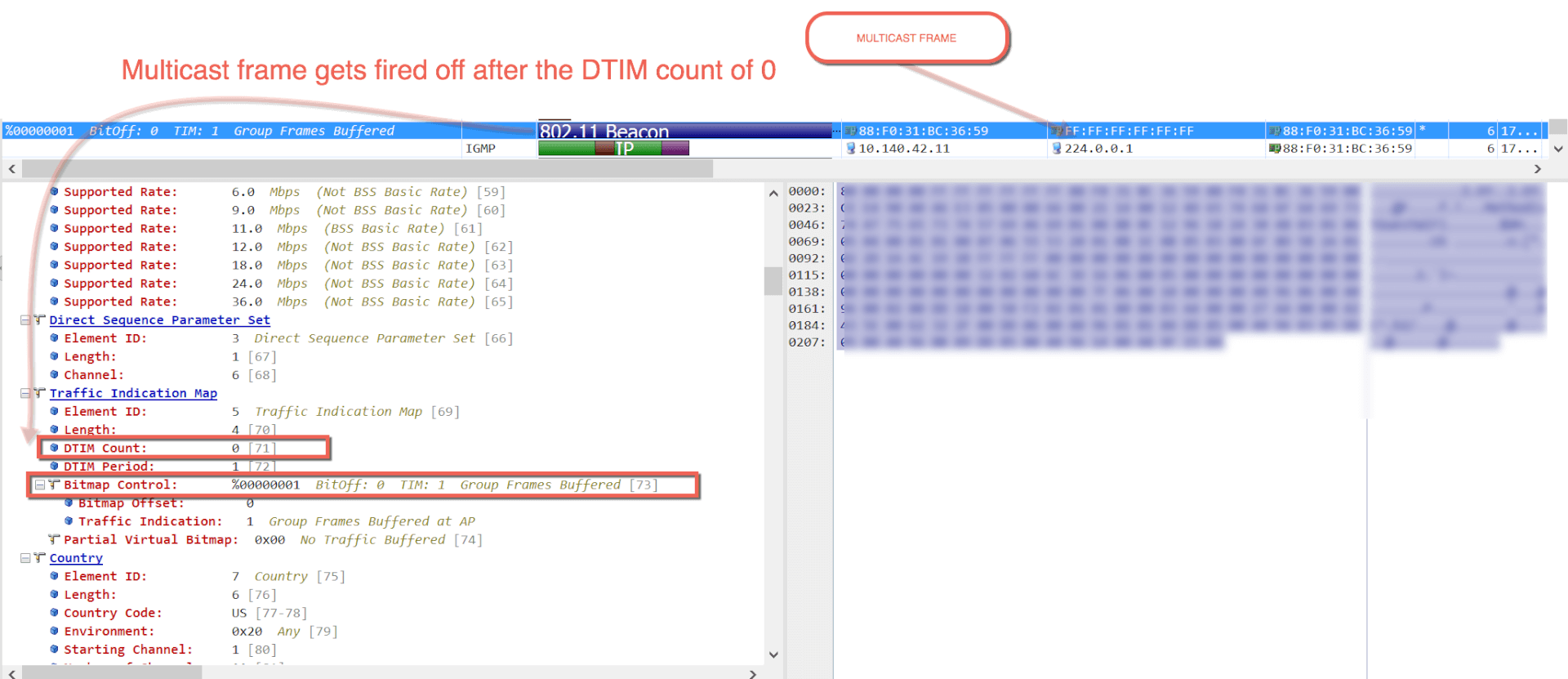
1. This field indicates the beacon intervals till a DTIM.
2. A DTIM period field of 1 indicates every other beacon is a DTIM.
3. A DTIM period field of 3 indicates every third beacon is a DTIM.
4. A DTIM period field of 5 indicates every fifth beacon is a DTIM.
5. When the first bit of the bitmap control field is set to 1 there is broadcast, or multicast traffic buffered at the access point.

**Example: BROADCAST / MULTICAST TRAFFIC BUFFERED**

**DTIM summary**

1. stations are aware of the DTIM transmission intervals when they process beacons.
2. They should awaken or stay awake for the DTIM.
3. DTIM broadcast / multicast traffic is immediately transmitted after the beacon with the DTIM count field of 0.

**Example:** A DTIM count of zero and a multicast frame being transmitted immediately afterwards.



Name: V. Raju

Emp ID: 46254505