

Powersave Test Cases

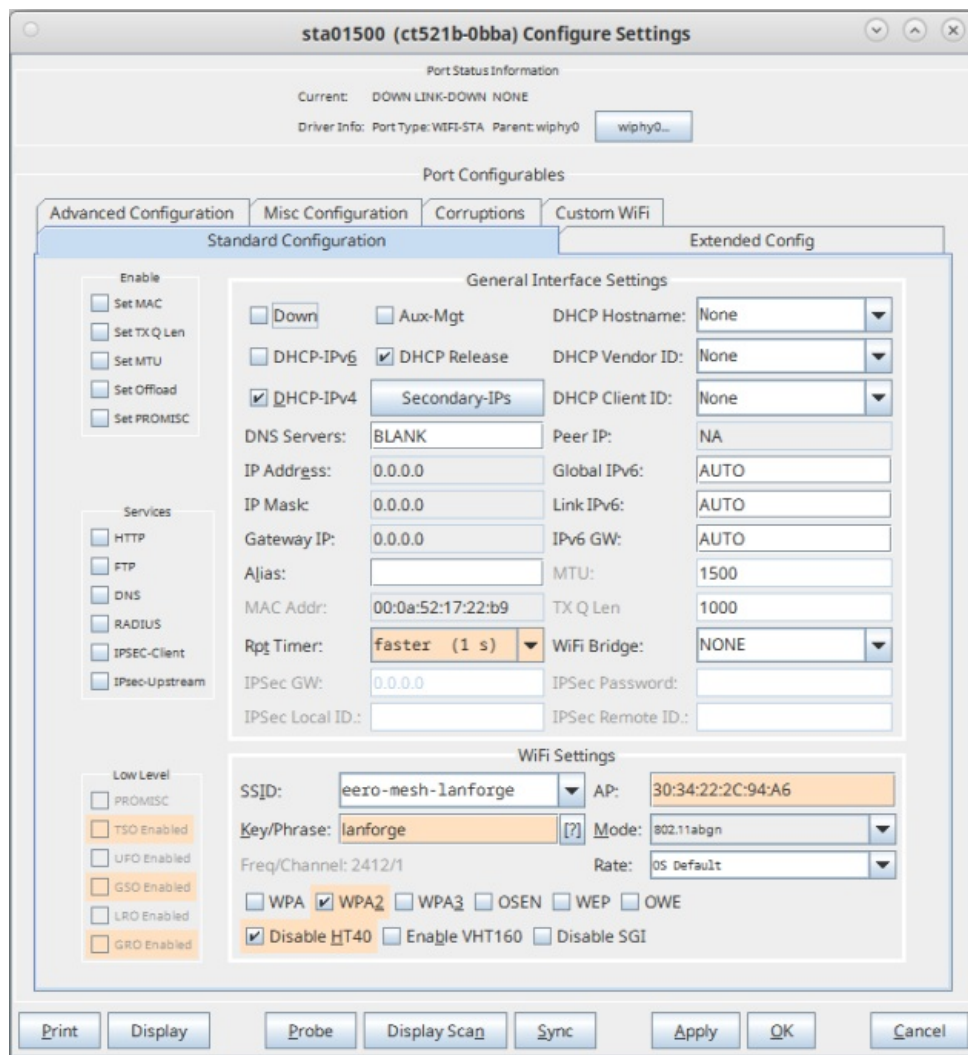
Goal: Test and verify powersave mode on a station using various methods.

DTIM multicast testing:

- Set up mcast traffic between upstream port sending to station with parameters of 9kbps Min Speed, 128 Kbps Max Speed and Default Pkt Size using the following cookbook link:
<http://www.candelatech.com/cookbook.php?vol=wifire&book=Wifi+Station+Multicast> .
- Double-click on the created station in the Port Mgr tab. Enable Powersave on LANforge station (in the Misc Configuration tab)

The screenshot shows the 'sta01500 (ct521b-0bba) Configure Settings' dialog box. The 'Misc Configuration' tab is selected, and the 'Powersave' checkbox is checked. The 'More WiFi Settings' section includes various configuration options such as TX-power, Preamble, NSS, OCSP, Freq-2.4, AMPDU-Factor, Max-AMSDU, X-Coordinate, Z-Coordinate, Post IF-UP Script, Custom WPA Cfg, WPA Cfg, Managed STA, IBSS Mode, MESH Mode, WDS Mode, Scan Hidden, Passive Scan, Allow Migration, Disable Fast Reauth, Restart DHCP on Connect, Skip Portal on Roam, No Auto ESS Roaming, No Apply DHCP, Disable Oper Class IE, BSS Transition, Disable TWT, Disable OFDMA, Disable OBSS Scan, Roam FT-DS, and Reject Beacon Req.

- Configure station for something easy to sniff (20Mhz a/b/g/n) by clicking the Disable HT40 button in the Standard Configuration tab. Then click Apply and OK to close the Configure Settings window for the station.



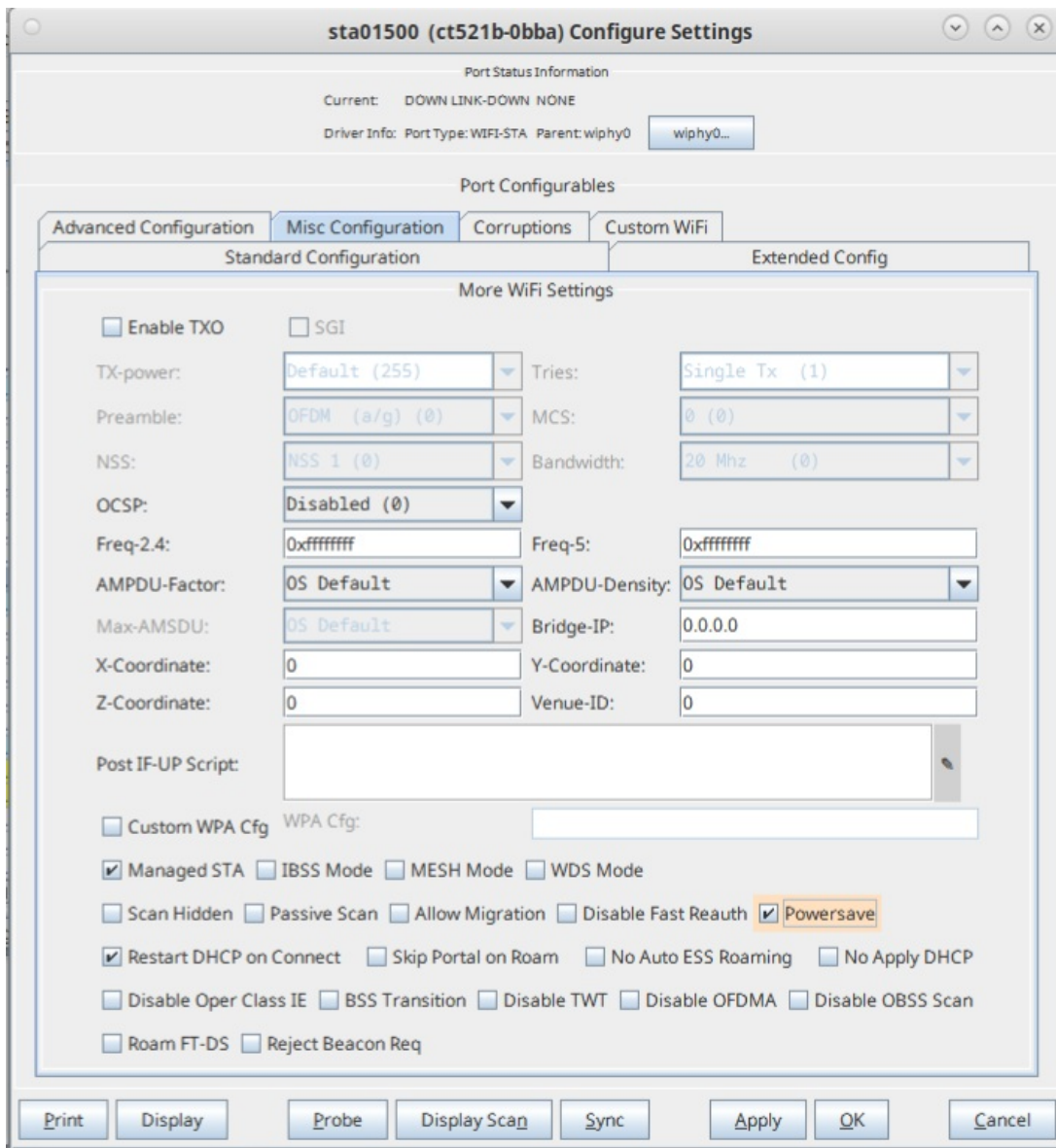
- Start sniffer with set mac filter to see all frames from AP BSSID or STA BSSID.
- Investigate packet capture:
 - The beacon right before the mcast frame should have the TIM Multicast flag set.
 - Beacon without mcast frame soon after should NOT have the Multicast flag set.
 - DTIM count counts down to zero, only at zero can mcast frames be transmitted.
 - DTIM count should count down, with maximum value being DTIM Period - 1.
 - If AP can change DTIM period, test with multiple DTIM periods.

This pcap file from a station on a mtk7921k radio shows proper unicast behavior. This is using the packet filter: wlan.addr == a8:93:4a:9d:47:a3 || wlan.addr == 04:f0:21:9a:64:65

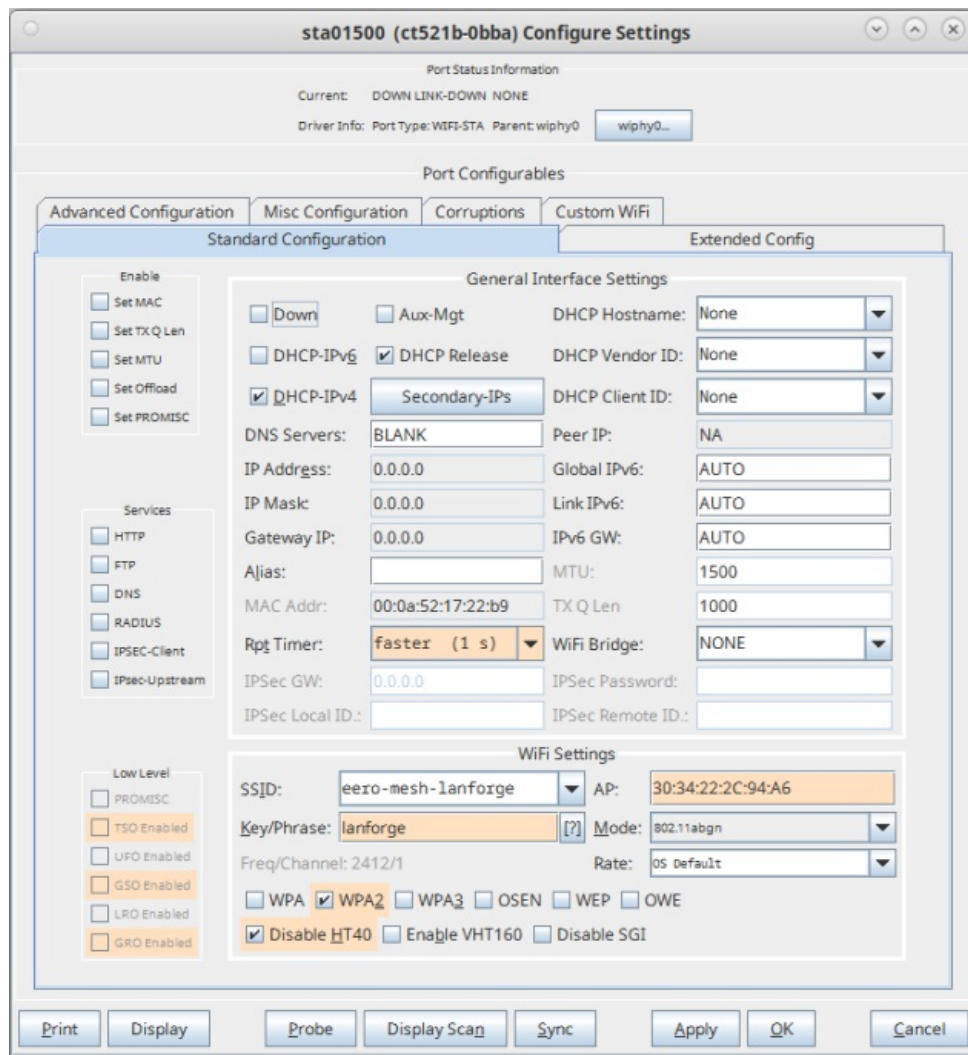
This pcap file shows bad broadcast Powersave behavior. Frame 157 TIM field should indicate Multicast and the broadcast frame 158 should be immediately after frame 157 instead of being 65ms later.

TIM unicast testing (with APs set up for multicast → unicast behaviour):

- Set up download unicast TCP traffic between upstream port and station. Set the Min Speed as 9 Kbps, Max Speed 128 Kbps, and 1400 as the Pkt Size.
- Double-click on the created station in the Port Mgr tab. Enable Powersave on LANforge station (in the Misc Configuration tab)



- Configure station for something easy to sniff (20Mhz a/b/g/n) by clicking the Disable HT40 button in the Standard Configuration tab. Then click Apply and OK to close the Configure Settings window for the station.



- Start sniffer, with optional filter to see all frames from AP BSSID or STA BSSID.
- Investigate packet capture:
 - The beacon should indicate that AID has traffic waiting (and Multicast flag would not be set).
 - STA should send wake-up null-func frame very soon after the beacon is seen (regardless of DTIM count/period, which is not pertinent for unicast frames).
 - AP acks that and proceeds to send queued traffic to STA.
 - STA goes back to sleep after a short period (around 100ms)
 - Average latency for the TCP download frames is around 100ms since frames are held on the AP until the next beacon so that STA can know to wake.

power-save-ax200-asus.pc...

power-save-ax200-sta-998...

power-save-mtk7921k-sta-...

For the ASUS capture above, use this filter for **ax200: wlan.addr == 50:e0:85:8a:0a:f2 || wlan.addr == F0:2F:74:7C:A3:B0**, for ax200 to LANforge VAP use: **wlan.addr == 50:e0:85:8a:0a:f2 || wlan.addr == wlan.addr == 04:f0:21:9a:64:65** and for the mtk to LANforge VAP, use: **wlan.addr == a8:93:4a:9d:47:a3 || wlan.addr == 04:f0:21:9a:64:65**

The ax200 capture shows buggy behaviour on the ASUS: ASUS does not ack frames well so ax200 sends lots of retries. The ASUS is doing multicast to unicast behaviour, so the 'multicast' frames are sent as directed unicast

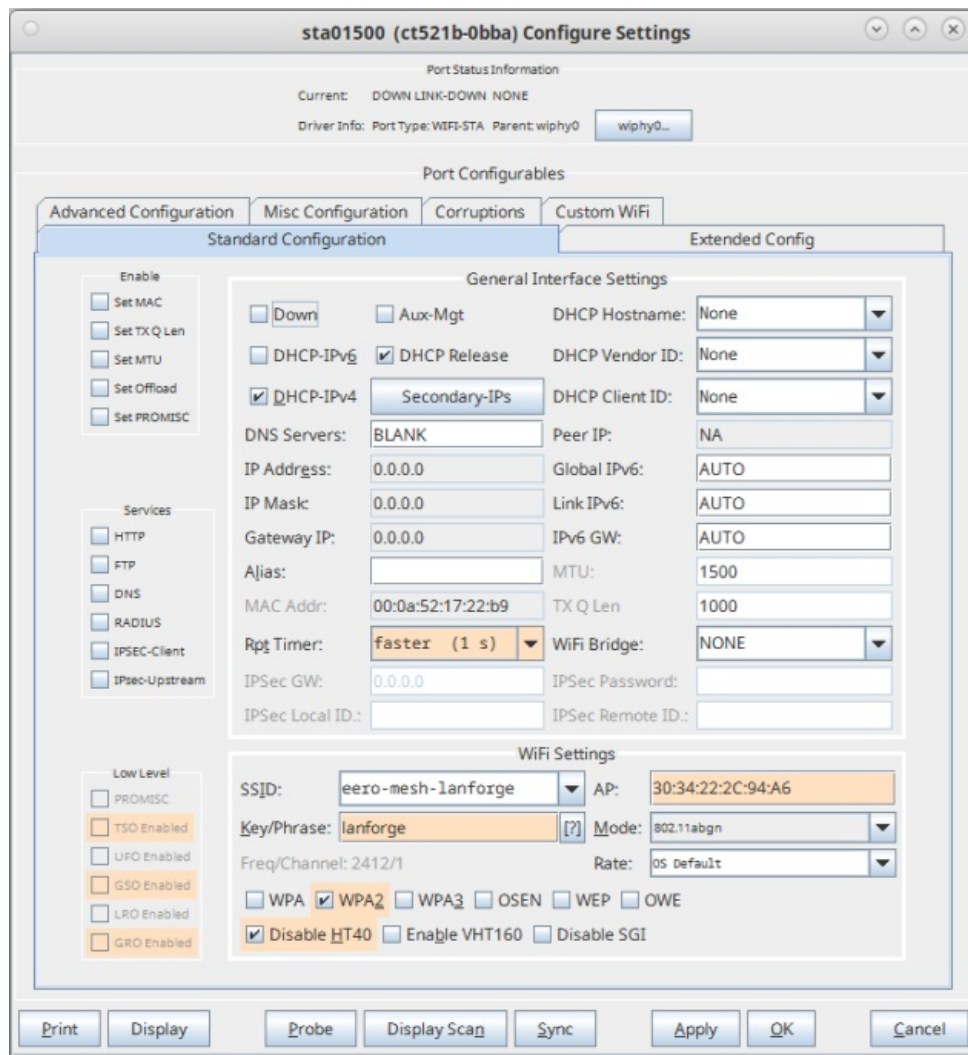
frames directly to the station.

Wake/Sleep testing in upload direction

- Set bursty traffic, min of zero, max of 128kbps, in upload direction.
- Double-click on the created station in the Port Mgr tab. Enable Powersave on LANforge station (in the Misc Configuration tab)

The screenshot shows the 'sta01500 (ct521b-0bba) Configure Settings' window. The 'Misc Configuration' tab is selected, and the 'More WiFi Settings' section is expanded. The 'Powersave' checkbox is checked and highlighted with an orange box. Other settings include 'Enable TXO' (unchecked), 'SGI' (unchecked), 'TX-power: Default (255)', 'Preamble: OFDM (a/g) (0)', 'NSS: NSS 1 (0)', 'OCSP: Disabled (0)', 'Freq-2.4: 0xffffffff', 'AMPDU-Factor: OS Default', 'Max-AMSDU: OS Default', 'X-Coordinate: 0', 'Z-Coordinate: 0', 'Post IF-UP Script' (empty), 'Custom WPA Cfg' (unchecked), 'WPA Cfg' (empty), 'Managed STA' (checked), 'IBSS Mode' (unchecked), 'MESH Mode' (unchecked), 'WDS Mode' (unchecked), 'Scan Hidden' (unchecked), 'Passive Scan' (unchecked), 'Allow Migration' (unchecked), 'Disable Fast Reauth' (unchecked), 'Restart DHCP on Connect' (checked), 'Skip Portal on Roam' (unchecked), 'No Auto ESS Roaming' (unchecked), 'No Apply DHCP' (unchecked), 'Disable Oper Class IE' (unchecked), 'BSS Transition' (unchecked), 'Disable TWT' (unchecked), 'Disable OFDMA' (unchecked), 'Disable OBSS Scan' (unchecked), 'Roam FT-DS' (unchecked), and 'Reject Beacon Req' (unchecked). The 'Apply' button is highlighted.

- Configure station for something easy to sniff (20Mhz a/b/g/n) by clicking the Disable HT40 button in the Standard Configuration tab. Then click Apply and OK to close the Configure Settings window for the station.

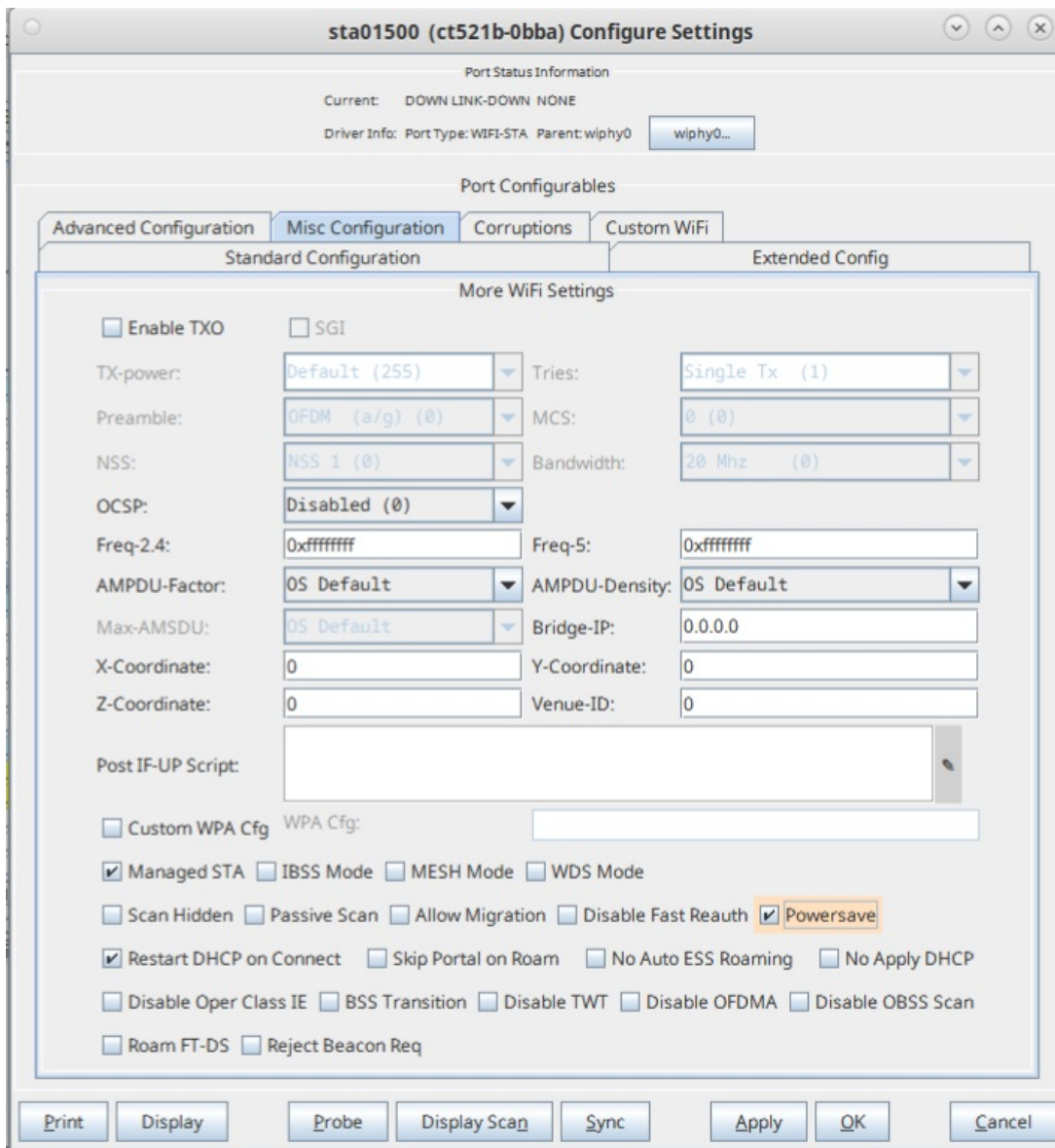


- Start sniffer, with optional filter to see all frames from AP BSSID or STA BSSID.
- Watch for packets from STA indicating it is going awake or asleep (Frame Control Field → Flags → PWR MGT)
- STA should :
 - indicate it is awake before transmitting frames.
 - go to sleep after a period of idle time (about 100ms, I think, but it may depend on the station).
 - not transmit while asleep
- STA may receive multicast packets while 'asleep' using the DTIM logic described above.
- AP should not transmit unicast frames to STA while STA is asleep.

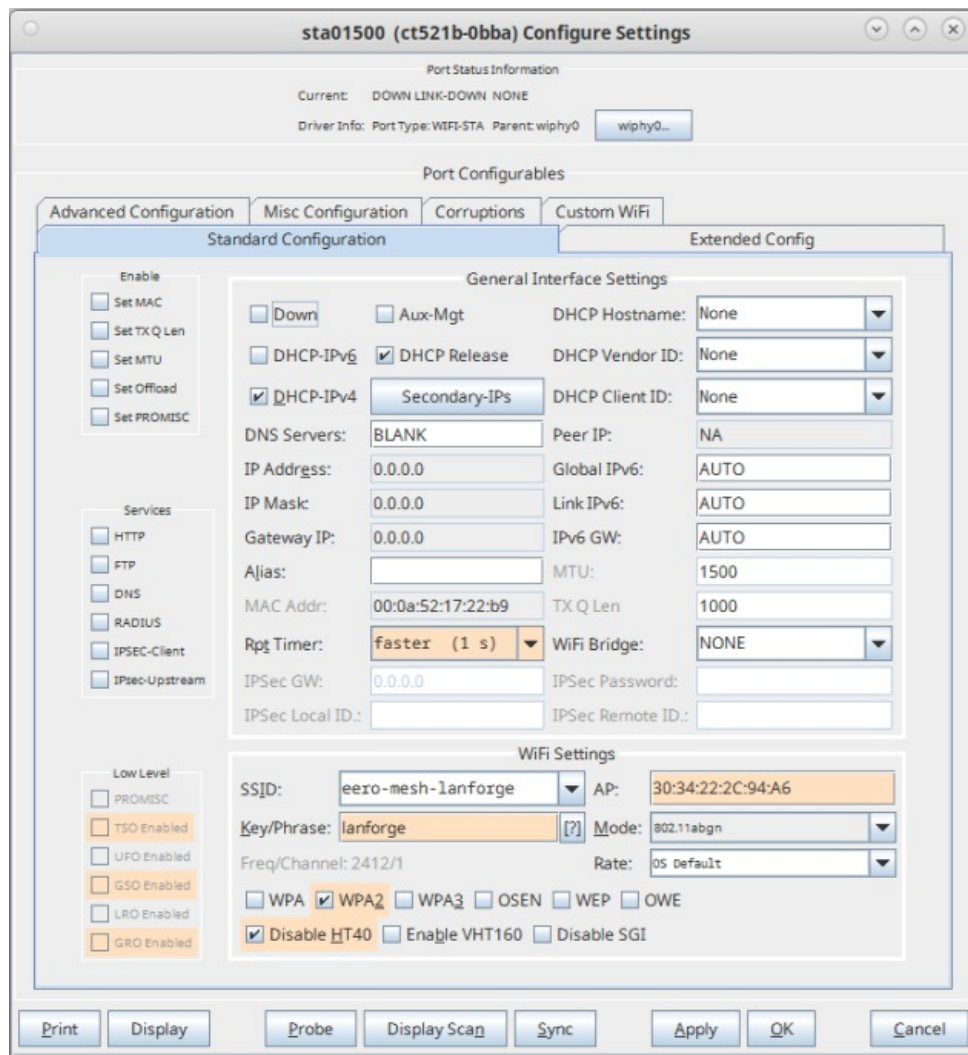
The following capture: shows power-save-mtk7921k-sta-mtk7915-lanforge-vap-unicast-upload.pcapng capture shows mtk7921k station talking to a LANforge mtk7915 VAP. The capture filter is: **wlan.addr == a8:93:4a:9d:47:a3 | | wlan.sa == 00:0A:52:46:8D:4**. The capture starts with the TCP traffic idle and the station in sleep mode. The STA then wakes up in frame 884 and it starts sending TCP traffic in frame 888. The TCP traffic has then quiesced for a bit in frame 996 and STA goes back to sleep.

Wake/Sleep testing in download direction

- Configure AP for bridge mode so that NAT is not an issue. Follow the following cookbook link to configure the AP in bridge mode: <http://www.candelatech.com/cookbook.php?vol=wifi&book=wifi+VAP+bridge>
- Double-click on the created station in the Port Mgr tab. Enable Powersave on LANforge station (in the Misc Configuration tab)



- Configure station for something easy to sniff (20Mhz a/b/g/n) by clicking the Disable HT40 button in the Standard Configuration tab. Then click Apply and OK to close the Configure Settings window for the station.

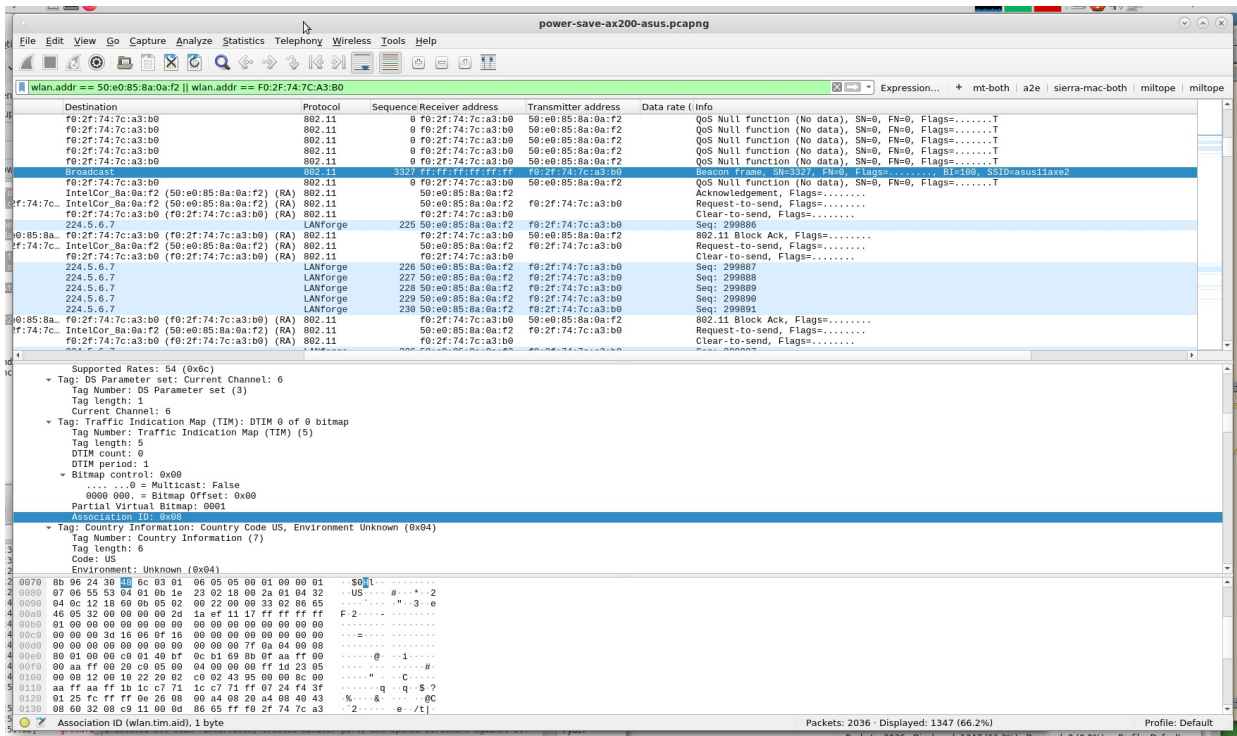


- Start sniffer, with optional filter to see all frames from AP BSSID or STA BSSID.
- Ping from upstream to STA, one packet per second.
- Ping latency should vary from near zero to the beacon interval since AP will store packets between when STA sleeps and wakes again. STA will wake after seeing indication in DTIM that it needs to receive (non multicast) frames.
- Packet loss should not be very high, this indicates AP is storing frames properly and that STA is waking properly.
- Ping from STA to upstream should not have much latency, because STA should wake each time it wants to send ICMP request, and stay awake long enough to receive the response before going back to sleep.

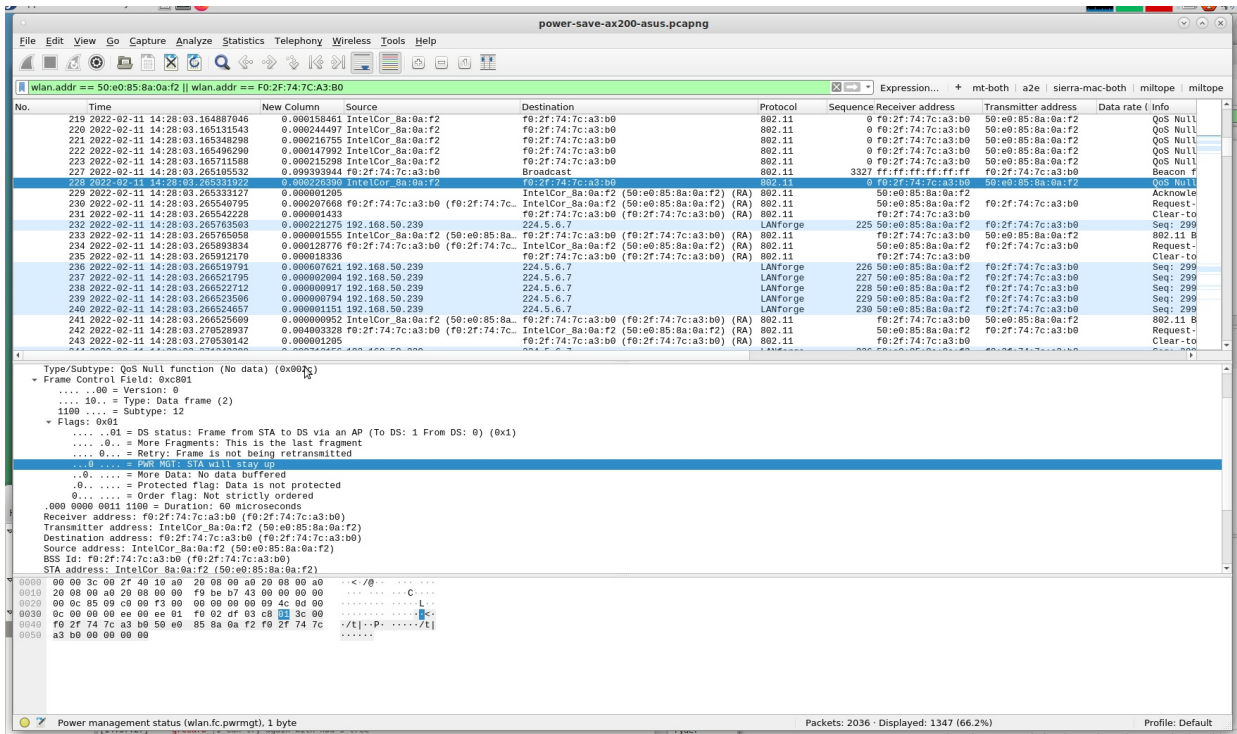
Packet Capture Analysis of Ucast to Mcast Capture with Buggy AP with Bad Ack on Frames

See 'power-save-ax200-asus.pcapng' file linked above. The captures 'power-save-ax200-sta-9984-lanforge-vap-unicast.pcapng' and 'power-save-mtk7921k-sta-9984-lanforge-vap-unicast.pcapng' show similar behaviour, but without the buggy lack of ACKs from the AP since a different AP (LANforge on QCA 9984 chipset) was used.

Starting with frame 227, a beacon frame, the AP indicates in the TIM IE that (unicast) data is waiting for the station with Association ID (AID) 0x8. This is the LANforge station in question, where it's AID is seen in the 'Probe' text dump in LANforge. This can also be seen by looking at the association frames, though this is not part of the capture. The TIM does not set the Multicast bit since this AP is converting multicast to unicast.



Frame 228 is from the station. It will always wake up to receive the beacon so that it can check the TIM element to see if it needs to stay awake and tell AP it needs to receive frames. Frame 228 is a few microseconds after the beacon, and STA tells the AP that it is waking up (because the AID was set in the TIM), and so AP can send traffic to it:



The multicast frames (converted to unicast in this case) are sent very soon after the STA wakes, see frames 232, 236 - 240. After the burst of multicast frames, the traffic goes quiet. The station decides to go back to sleep at frame 259. Notice the interval between frames, and that it has been idle for a bit...

The screenshot shows a Wireshark interface with a packet capture filter: `wlan.addr == 50:e0:85:8a:0a:f2 || wlan.addr == f0:2f:74:7c:a3:b0`. The packet list pane shows multiple entries, with packet 269 highlighted. The packet details pane for packet 269 shows:

- ... 10... = Type: Data Frame (2)
- 1100 ... = Subtype: 12
- Flags: 0x11
-01 = DS status: Frame from STA to DS via an AP (To DS: 1 From DS: 0) (0x1)
-0 = More Fragments: This is the last fragment
-0... = Retry: Frame is not being retransmitted
-0... = Protected flag: Data is not protected
-0... = Order flag: Not strictly ordered
-000 0000 0011 1100 = Duration: 60 microseconds
- Receiver address: f0:2f:74:7c:a3:b0 (f0:2f:74:7c:a3:b0)
- Transmitter address: IntelCor_8a:0a:f2 (50:e0:85:8a:0a:f2)
- Destination address: f0:2f:74:7c:a3:b0 (f0:2f:74:7c:a3:b0)
- Source address: IntelCor_8a:0a:f2 (50:e0:85:8a:0a:f2)
- BSS ID: f0:2f:74:7c:a3:b0 (f0:2f:74:7c:a3:b0)
- STA address: IntelCor_8a:0a:f2 (50:e0:85:8a:0a:f2)
-0000 0000 = Fragment number: 0
-0000 0000 0000 = Sequence number: 0
- QoS Control: 0x0000

The packet bytes pane shows the raw data: `0000 00 00 3c 00 2f 40 10 a0 20 08 00 a0 20 08 00 a0` and so on.

Packet Capture Analysis of Multicast Capture with Powersave

See file 'power-save-mtk7921k-sta-9984-lanforge-vap.pcapng', using filter: `wlan.addr == a8:93:4a:9d:47:a3 || wlan.addr == 04:f0:21:9a:64:65`

The AP in this setup is LANforge using QCA 9984 chipset radio. The AP is not set to convert multicast to unicast, so we get to inspect how multicast traffic is queued and sent to sleeping stations.

In frame 269, the station goes to sleep. It does not wake up again, at least not often, but it does wake up to hear beacons and pay attention to the DTIM so it can stay awake to receive multicast frames when needed. This was verified by ensuring that the multicast receiver endpoint on the station shows proper amount of received traffic.

*moni3a (on ct523c-0b29)

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

wlan.addr == a8:93:4a:9d:47:a3 || wlan.addr == 04:f0:21:9a:64:65

No.	Time	Source	Destination	Protocol	Length	PPDU Format	Type/Subtype	AID12
258	2.457651623	CompexPt_9a:64:65	Broadcast	802.11	248		Beacon frame	
267	2.565869912	a8:93:4a:9d:47:a3 (a8:93:4a:9d:47:a3) (TA)	CompexPt_9a:64:65 (04:f0:21:9a:64:65)	802.11	76		Request-to-send	
268	2.565891416	a8:93:4a:9d:47:a3	a8:93:4a:9d:47:a3 (a8:93:4a:9d:47:a3)	802.11	70		Clear-to-send	
269	2.566025246	a8:93:4a:9d:47:a3	CompexPt_9a:64:65	802.11	84		Null function (No data)	
270	2.566052042	a8:93:4a:9d:47:a3	a8:93:4a:9d:47:a3 (a8:93:4a:9d:47:a3)	802.11	70		Acknowledgement	
284	2.703411152	CompexPt_9a:64:65	Broadcast	802.11	248		Beacon frame	
285	2.705508437	172.16.223.153	224.6.6.6	LANfor_	1592		Data	
310	2.949171336	CompexPt_9a:64:65	Broadcast	802.11	248		Beacon frame	
318	3.031863685	CompexPt_9a:64:65	SparkLAN_4e:58:c1	802.11	242		Probe Response	
319	3.032252920	CompexPt_9a:64:65	SparkLAN_4e:58:c1	802.11	242		Probe Response	
320	3.032639366	CompexPt_9a:64:65	SparkLAN_4e:58:c1	802.11	242		Probe Response	
321	3.033029663	CompexPt_9a:64:65	SparkLAN_4e:58:c1	802.11	242		Probe Response	
338	3.194881874	CompexPt_9a:64:65	Broadcast	802.11	248		Beacon frame	
339	3.197038423	172.16.223.153	224.6.6.6	LANfor_	1592		Data	
340	3.199194556	172.16.223.153	224.6.6.6	LANfor_	1592		Data	
364	3.448818649	CompexPt_9a:64:65	Broadcast	802.11	248		Beacon frame	

```

.... 00 = Version: 0
.... 10.. = Type: Data frame (2)
0100 .... = Subtype: 4
  Flags: 0x11
    .... 01 = DS status: Frame from STA to DS via an AP (To DS: 1 From DS: 0) (0x1)
    .... 0.. = More Fragments: This is the last fragment
    .... 0... = Retry: Frame is not being retransmitted
    ...1 .... = PWR Mgt: STA will go to sleep
    ..0. .... = More Data: No data buffered
    0.. .... = Protected flag: Data is not protected
    0... .... = Order Flag: Not strictly ordered
    000 0000 0010 0100 = Duration: 36 microseconds
Receiver address: CompexPt_9a:64:65 (04:f0:21:9a:64:65)
Transmitter address: a8:93:4a:9d:47:a3 (a8:93:4a:9d:47:a3)
Destination address: CompexPt_9a:64:65 (04:f0:21:9a:64:65)
Source address: a8:93:4a:9d:47:a3 (a8:93:4a:9d:47:a3)
BSS Id: CompexPt_9a:64:65 (04:f0:21:9a:64:65)
STA address: a8:93:4a:9d:47:a3 (a8:93:4a:9d:47:a3)
..... 0000 = Fragment number: 0
0000 0100 1111 .... = Sequence number: 79

0000 00 00 3c 00 2f 40 10 a0 20 08 00 a0 20 08 00 a0  ..< /@ ..
0010 20 08 00 a0 20 08 00 00 10 59 4d 30 00 00 00 00  .. . . . . YMO .
0020 00 0c 3c 14 40 01 d6 00 00 00 00 00 dc eb 10 00  ..< @ ..
0030 0c 00 00 00 d6 00 d1 01 03 02 cf 03 48 24 00 00  .. . . . . HSS .
0040 04 f0 21 9a 64 65 a8 93 4a 9d 47 a3 04 f0 21 9a  ..! de . . J-G . .
0050 64 65 f0 04  .. de . .

```

Power management status (wlan.fc.pwrmtg), 1 byte(s) Packets: 618 · Displayed: 52 (8.4%) · Dropped: 0 (0.0%) Profile: Default

Frame 364 shows DTIM with no multicast bit set, indicating no mcast frames are queued. And, DTIM count is 1, which means that stations do not need to wake now, but do need to wake for next DTIM period.

The screenshot shows a Wireshark capture window titled '*moni3a (on ct523c-0b29)'. The interface includes a menu bar (File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, Help) and a toolbar. The packet list pane at the top displays a series of packets, with packet 365 selected. The details pane for packet 365 shows the following structure:

- Supported Rates: 12(B) (0x98)
- Supported Rates: 18 (0x24)
- Supported Rates: 24(B) (0xb0)
- Supported Rates: 36 (0x48)
- Supported Rates: 48 (0x60)
- Supported Rates: 54 (0x6c)
- Tag: DS Parameter set: Current Channel: 36
 - Tag Number: DS Parameter set (3)
 - Tag length: 1
 - Current Channel: 36
- Tag: Traffic Indication Map (TIM): DTIM 1 of 0 bitmap
 - Tag Number: Traffic Indication Map (TIM) (5)
 - Tag length: 4
 - DTIM count: 1
 - DTIM period: 2
 - Bitmap control: 0x00
 - ... 0 = Multicast: False
 - 0000 0000 = Bitmap Offset: 0x00
 - Partial Virtual Bitmap: 00
 - Tag: Supported Operating Classes
 - Tag Number: Supported Operating Classes (59)

The raw packet data pane at the bottom shows the hexadecimal and ASCII representation of the packet bytes, starting with 0000 00 00 3c 06 2f 40 10 a0 20 08 00 a0 20 08 00 a0.

Indicates how many Beacon frames (including the current frame before the next DTIM (wlan.tim.dtim_count), 1 byte(s) Packets: 618 - Displayed: 52 (8.4%) - Dropped: 0 (0.0%) Profile: Default

Frame 365 is next beacon, and it shows mcast frames are queued, and the DTIM count indicates that stations should wake NOW to receive the queued frames.

The image shows a Wireshark packet capture window titled '*moni3a (on ct523c-0b29)'. The interface includes a menu bar (File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, Help) and a toolbar. A filter bar at the top shows 'wlan.addr == a8:93:4a:9d:47:a3 || wlan.addr == 04:f0:21:9a:64:65'. The packet list pane displays a series of packets, with packet 387 selected. The packet details pane shows the structure of a beacon frame, including supported rates (12(B) (0x98), 18 (0x24), 24(B) (0xb0), 36 (0x48), 48 (0x60), 54 (0x6c)), a DS Parameter set (Current Channel: 36), a Traffic Indication Map (TIM) (DTIM 0 of 1 bitmap), and supported operating classes (59). The packet bytes pane shows the raw data of the selected packet in hexadecimal and ASCII.

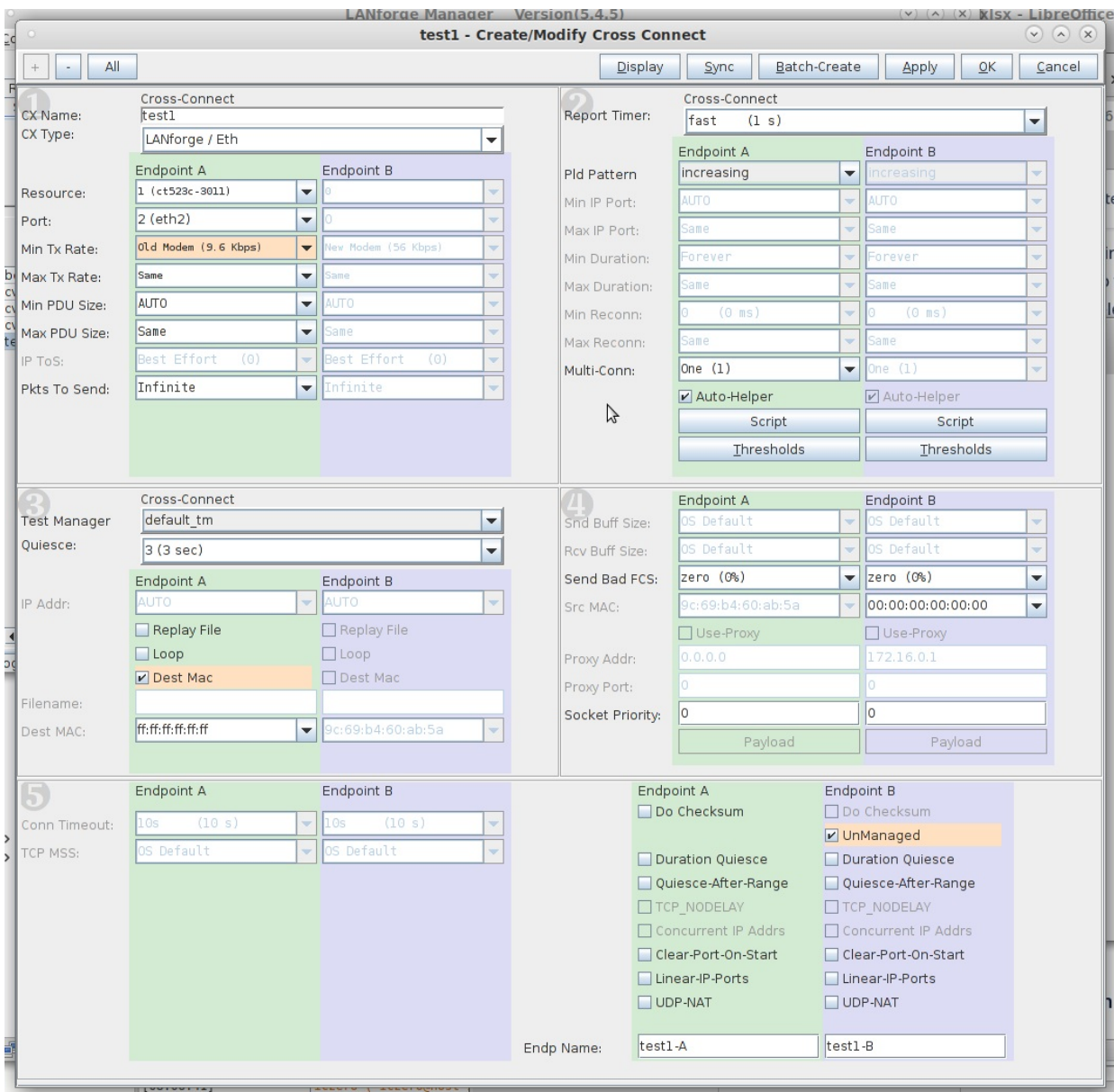
No.	Time	Source	Destination	Protocol	Length	PPDU Format	Type/Subtype	AID12
285	2.705508437	172.16.223.153	224.6.6.6	LANfor_	1592		Data	
310	2.949171336	CompexPT_9a:64:65	Broadcast	802.11	248		Beacon frame	
318	3.031863685	CompexPT_9a:64:65	SparkLAN_4e:58:c1	802.11	242		Probe Response	
319	3.032252020	CompexPT_9a:64:65	SparkLAN_4e:58:c1	802.11	242		Probe Response	
320	3.032639366	CompexPT_9a:64:65	SparkLAN_4e:58:c1	802.11	242		Probe Response	
321	3.033029663	CompexPT_9a:64:65	SparkLAN_4e:58:c1	802.11	242		Probe Response	
338	3.194881874	CompexPT_9a:64:65	Broadcast	802.11	248		Beacon frame	
339	3.197038423	172.16.223.153	224.6.6.6	LANfor_	1592		Data	
340	3.199194556	172.16.223.153	224.6.6.6	LANfor_	1592		Data	
364	3.440818649	CompexPT_9a:64:65	Broadcast	802.11	248		Beacon frame	
387	3.686459396	CompexPT_9a:64:65	Broadcast	802.11	248		Beacon frame	
388	3.688557092	172.16.223.153	224.6.6.6	LANfor_	1592		Data	
410	3.932218491	CompexPT_9a:64:65	Broadcast	802.11	248		Beacon frame	
436	4.177984526	CompexPT_9a:64:65	Broadcast	802.11	248		Beacon frame	
437	4.180085762	172.16.223.153	224.6.6.6	LANfor_	1592		Data	
450	4.423743628	CompexPT_9a:64:65	Broadcast	802.11	248		Beacon frame	

And right after the beacon, the mcast frame is sent, as expected. Later, if station needs to send a frame, it would send a Null-Func frame with the 'STA is awake' flag set, and if AP needed to send a unicast frame, the AID of the STA would be added to the TIM element and so STA would wake for that as well....

Packet capture for buggy broadcast power-save behavior:

See file linked near the top: bad-bcast-powersave.pcapng

LANforge is configured to generate slow broadcast traffic in downstream direction using LANforge-Eth layer-3 connection type, with Dest Mac specified as all FFs, and 'b' side as un-managed. This causes A side to blindly send out these frames, the B side does not actually attempt to receive it.



This AP is not buffering broadcast packets and sending them after the beacon like it is supposed to. Frame 157 (beacon) does not have Multicast bit set in its TIM:

The screenshot shows a Wireshark capture of IEEE 802.11 wireless LAN traffic. The packet list pane displays a series of frames from 154 to 175. Packet 158 is highlighted in blue, indicating it is the selected packet. The packet details pane shows the structure of the IEEE 802.11 frame, including MAC addresses, SSID, and other parameters.

No.	Time	New Column	Source	Destination	Protocol	Sequence/Receiver address	Transmitter address	Data rate (Info)	Info
154	2022-02-25 08:52:53.117098829	0.992032622	14:16:9d:53:58:ce	Broadcast	802.11	274 ff:ff:ff:ff:ff:ff	14:16:9d:53:58:ce	Beacon F	
155	2022-02-25 08:52:53.117795908	0.990697079	14:16:9d:53:58:cf	Broadcast	802.11	2429 ff:ff:ff:ff:ff:ff	14:16:9d:53:58:cf	Beacon F	
156	2022-02-25 08:52:53.127699949	0.999164564	68:7d:b4:5f:5c:3f	Broadcast	802.11	2574 ff:ff:ff:ff:ff:ff	68:7d:b4:5f:5c:3f	Beacon F	
157	2022-02-25 08:52:53.127558666	0.990598174	68:7d:b4:5f:5c:3e	Broadcast	802.11	1872 ff:ff:ff:ff:ff:ff	68:7d:b4:5f:5c:3e	Beacon F	
158	2022-02-25 08:52:53.192883681	0.99525615	Shenzhen_ab5a	Broadcast	802.11	2312 ff:ff:ff:ff:ff:ff	68:7d:b4:5f:5c:3e	Data, SN	
159	2022-02-25 08:52:53.219495042	0.920611361	14:16:9d:53:58:ce	Broadcast	802.11	275 ff:ff:ff:ff:ff:ff	14:16:9d:53:58:ce	Beacon F	
160	2022-02-25 08:52:53.220195540	0.990706498	14:16:9d:53:58:cf	Broadcast	802.11	2430 ff:ff:ff:ff:ff:ff	14:16:9d:53:58:cf	Beacon F	
161	2022-02-25 08:52:53.229361637	0.999166997	68:7d:b4:5f:5c:3f	Broadcast	802.11	2575 ff:ff:ff:ff:ff:ff	68:7d:b4:5f:5c:3f	Beacon F	
162	2022-02-25 08:52:53.229961637	0.990099704	68:7d:b4:5f:5c:3e	Broadcast	802.11	1973 ff:ff:ff:ff:ff:ff	68:7d:b4:5f:5c:3e	Beacon F	
163	2022-02-25 08:52:53.321896733	0.991935392	14:16:9d:53:58:ce	Broadcast	802.11	276 ff:ff:ff:ff:ff:ff	14:16:9d:53:58:ce	Beacon F	
164	2022-02-25 08:52:53.322599927	0.990702294	14:16:9d:53:58:cf	Broadcast	802.11	2431 ff:ff:ff:ff:ff:ff	14:16:9d:53:58:cf	Beacon F	
165	2022-02-25 08:52:53.331761746	0.999162719	68:7d:b4:5f:5c:3f	Broadcast	802.11	2576 ff:ff:ff:ff:ff:ff	68:7d:b4:5f:5c:3f	Beacon F	
166	2022-02-25 08:52:53.332362381	0.990660635	68:7d:b4:5f:5c:3e	Broadcast	802.11	1874 ff:ff:ff:ff:ff:ff	68:7d:b4:5f:5c:3e	Beacon F	
167	2022-02-25 08:52:53.424273126	0.991910745	14:16:9d:53:58:ce	Broadcast	802.11	277 ff:ff:ff:ff:ff:ff	14:16:9d:53:58:ce	Beacon F	
168	2022-02-25 08:52:53.424905569	0.990632443	14:16:9d:53:58:cf	Broadcast	802.11	2432 ff:ff:ff:ff:ff:ff	14:16:9d:53:58:cf	Beacon F	
169	2022-02-25 08:52:53.434162252	0.999256683	68:7d:b4:5f:5c:3f	Broadcast	802.11	2577 ff:ff:ff:ff:ff:ff	68:7d:b4:5f:5c:3f	Beacon F	
170	2022-02-25 08:52:53.434763883	0.990690831	68:7d:b4:5f:5c:3e	Broadcast	802.11	1875 ff:ff:ff:ff:ff:ff	68:7d:b4:5f:5c:3e	Beacon F	
171	2022-02-25 08:52:53.527619788	0.991955042	14:16:9d:53:58:ce	Broadcast	802.11	278 ff:ff:ff:ff:ff:ff	14:16:9d:53:58:ce	Beacon F	
172	2022-02-25 08:52:53.527327225	0.990629100	14:16:9d:53:58:cf	Broadcast	802.11	2433 ff:ff:ff:ff:ff:ff	14:16:9d:53:58:cf	Beacon F	
173	2022-02-25 08:52:53.527563629	0.990236404	CompexPT_64-bb-69	68:7d:b4:5f:5c:3e	802.11	7 68:7d:b4:5f:5c:3e	64:f0:21:64:bb:69	NULL Fun	
174	2022-02-25 08:52:53.527651788	0.990698151	68:7d:b4:5f:5c:3f	CompexPT_64-bb-69 (RA)	802.11	04:f0:21:64:bb:69	68:7d:b4:5f:5c:3f	Acknowle	
175	2022-02-25 08:52:53.536489913	0.990883813	68:7d:b4:5f:5c:3f	Broadcast	802.11	2578 ff:ff:ff:ff:ff:ff	68:7d:b4:5f:5c:3f	Beacon F	

The packet details pane for packet 158 shows the following structure:

- IEEE 802.11 wireless LAN
 - Fixed parameters (12 bytes)
 - Tag: SSID parameter set: ssid_wpa2_5g
 - Tag: Supported Rates (6(B), 9, 12(B), 18, 24(B), 36, 48)54, [Mbit/sec]
 - Tag: DS Parameter set: Current Channel: 36
 - Tag: Traffic Indication Map (TIM) DTIM of ef 0 bitmap
 - Tag Number: Traffic Indication Map (TIM) (5)
 - Tag length: 4
 - DTIM count: 0
 - DTIM period: 1
 - Bitmap control: 0x00
 - 0 = Multicast; False
 - 0000 0000 = Bitmap Offset: 0x00
 - Partial Virtual Bitmap: 00
 - Tag: Country Information: Country Code US, Environment Unknown (0x04)
 - Tag: Power Constraint: 3
 - Tag: TPC Report: Transmit Power: 16, Link Margin: 0
 - Tag: RSN Information
 - 00 00 38 00 2f 40 40 a0 20 08 00 a0 20 08 00 00
 - 00 00 00 00 00 00 00 00 0f a4 70 00 00 00 00
 - 00 00 16 00 11 03 cd 00 cf 01 80 00 00 00 ff ff ff
 - 00 00 ff ff 68 7d b4 5f 5c 3e 68 7d b4 5f 5c 3e 80 75
 - 00 00 ff 52 05 05 00 00 64 00 11 15 00 8c 73 78
 - 00 00 69 64 5f 77 70 61 32 5f 35 67 01 08 8c 12 08 24
 - 00 00 b0 48 60 6c 03 01 24 95 04 00 01 00 09 67 4e 55
 - 00 00 53 04 24 01 18 20 01 18 20 01 18 34 04 04
 - 00 00 12 38 01 12 3c 01 12 40 01 12 64 01 12 68 01 13
 - 00 00 6c 01 13 70 01 13 74 01 13 78 01 13 7c 01 13 80
 - 00 00 01 13 84 01 13 88 01 13 8c 01 12 90 01 12 95 00
 - 00 00 1a 99 01 1a 9d 01 1a a1 01 1a a5 01 1a 20 01 03

Frame 158 (broadcast frame) arrives 65ms after the beacon, indicating that the AP did not buffer the frame properly.

The screenshot shows a Wireshark capture of a frame 158 bytes on wire. The packet details pane shows the structure of the frame, including MAC addresses, SSID, and other parameters.

Frame 158: 1594 bytes on wire (12752 bits), 1594 bytes captured (12752 bits) on interface 0

- RadioTap Header v0, Length 50
- 802.11 radio information
- IEEE 802.11 Data, Flags: p...F.C
 - Type/Subtype: Data (0x0000)
 - Frame Control Field: 0x0842
 - Receiver address: Broadcast (ff:ff:ff:ff:ff:ff)
 - Transmitter address: 68:7d:b4:5f:5c:3e (68:7d:b4:5f:5c:3e)
 - Destination address: Broadcast (ff:ff:ff:ff:ff:ff)
 - Source address: Shenzhen_ab5a (0c:69:b4:60-ab:5a)
 - BSS Id: 68:7d:b4:5f:5c:3e (68:7d:b4:5f:5c:3e)
 - STA address: Broadcast (ff:ff:ff:ff:ff:ff)
 - Sequence number: 0
 - Fragment number: 0
 - Sequence number: 2312
 - Frame check sequence: 0xbbaac33 [unverified]
 - [FCS Status: Unverified]
 - CCMP parameters
 - Data (1502 bytes)
 - 0000 00 00 38 00 2f 40 40 a0 20 08 00 a0 20 08 00 00
 - 00 00 00 00 00 00 00 00 00 ac 9d 7a 00 00 00 00 00
 - 00 00 16 00 11 03 cd 00 cf 01 80 42 00 00 ff ff ff
 - 00 00 ff ff 68 7d b4 5f 5c 3e 68 7d b4 5f 5c 3e 80 75
 - 00 00 68 09 00 00 00 00 00 06 d5 6f 03 e5 42 c9 ac
 - 00 00 a9 ac e2 0e 64 a2 72 96 da 5e f5 e8 5d 48 21 ca
 - 00 00 01 04 e2 0e 5a 1f 53 00 75 a7 c7 62 c2 84 6d fe
 - 00 00 45 c8 08 95 1e 92 ba 67 90 45 b3 0a 10 25 0e 70
 - 00 00 1e 1e a2 11 12 ac 60 15 c3 54 a2 b9 58 68 48
 - 00 00 55 3b 6f 07 e1 7b 8f db dc 07 2e 73 09 99 99 2f
 - 00 00 a7 5b 0f c8 fa 4b 46 52 f1 41 07 02 46 89 ab ec
 - 00 00 83 e9 44 95 12 ac 18 ed 28 3c 08 31 22 68 38 66

Packet capture for Wake/Sleep testing in upload direction:

See file 'power-save-mtk7921k-sta-mtk7915-lanforge-vap-unicast-upload.pcapng' This capture shows mtk7921k station talking to LANforge mtk7915 VAP. The capture filter is: **wlan.addr == a8:93:4a:9d:47:a3 || wlan.sa == 00:0A:52:46:8D:4**. The capture starts with the TCP traffic idle and the station in sleep mode. Frame 884 is STA waking up, and it starts sending TCP traffic frame 888.

power-save-mtk7921k-sta-mtk7915-lanforge-vap-unicast-upload.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

wlan_addr == a8:93:4a:9d:47:a3 | wlan_sa == 00:0A:52:46:8D:49

No.	Time	Source	Destination	Protocol	Length	Data rate	PHY type	Sequence number	Info
836	7.529672485	AsiarF_46:8d:49	Broadcast	802.11	330		6 802.11a (OFDM)		2975 Beacon frame, SN=2975, FN=0, Flags=....., BI=
853	7.775416041	AsiarF_46:8d:49	Broadcast	802.11	330		6 802.11a (OFDM)		2976 Beacon frame, SN=2976, FN=0, Flags=....., BI=
875	8.021210907	AsiarF_46:8d:49	Broadcast	802.11	330		6 802.11a (OFDM)		2977 Beacon frame, SN=2977, FN=0, Flags=....., BI=
878	8.112089974	Chongqin_9d:47:a3 (- AsiarF_46:8d:49)	Chongqin_9d:47:a3 (- AsiarF_46:8d:49)	802.11	70		24 802.11a (OFDM)		Clear-to-send, Flags=.....
885	8.112089902	Chongqin_9d:47:a3 (- AsiarF_46:8d:49)	Chongqin_9d:47:a3 (- AsiarF_46:8d:49)	802.11	70		24 802.11a (OFDM)		Request-to-send, Flags=.....
886	8.112440243	Chongqin_9d:47:a3 (- AsiarF_46:8d:49)	Chongqin_9d:47:a3 (- AsiarF_46:8d:49)	802.11	70		24 802.11a (OFDM)		Clear-to-send, Flags=.....
887	8.112440243	Chongqin_9d:47:a3 (- AsiarF_46:8d:49)	Chongqin_9d:47:a3 (- AsiarF_46:8d:49)	802.11	70		24 802.11a (OFDM)		Request-to-send, Flags=.....
888	8.112651462	172.16.223.154	172.16.223.153	LANFor	1590		104 802.11n (HT)		16 Seq: 1
889	8.112653310	172.16.223.154	172.16.223.153	TCP	162		104 802.11n (HT)		17 33033 - 33034 [PSH, ACK] Seq=1449 Ack=1 Win=42 L
890	8.112653887	AsiarF_46:8d:49 (00:0A:52:46:8D:49)	Chongqin_9d:47:a3 (- AsiarF_46:8d:49)	802.11	88		24 802.11a (OFDM)		802.11 Block Ack, Flags=.....
891	8.113396963	Chongqin_9d:47:a3 (- AsiarF_46:8d:49)	Chongqin_9d:47:a3 (- AsiarF_46:8d:49)	802.11	70		6 802.11a (OFDM)		Request-to-send, Flags=.....
892	8.113396938	Chongqin_9d:47:a3 (- AsiarF_46:8d:49)	Chongqin_9d:47:a3 (- AsiarF_46:8d:49)	802.11	70		6 802.11a (OFDM)		Clear-to-send, Flags=.....
893	8.113492971	AsiarF_46:8d:49	AsiarF_46:8d:49	802.11	86		6 802.11a (OFDM)		77 QoS Null function (No data), SN=77, FN=0, Flags=
894	8.113494712	Chongqin_9d:47:a3 (- AsiarF_46:8d:49)	Chongqin_9d:47:a3 (- AsiarF_46:8d:49)	802.11	70		6 802.11a (OFDM)		Acknowledgement, Flags=.....
895	8.113804233	172.16.223.154	172.16.223.153	TCP	150		39 802.11n (HT)		8 33034 - 33033 [ACK] Seq=1 Ack=1461 Win=41 Len=0
896	8.113805857	Chongqin_9d:47:a3 (- AsiarF_46:8d:49)	AsiarF_46:8d:49 (00:0A:52:46:8D:49)	802.11	88		6 802.11a (OFDM)		802.11 Block Ack, Flags=.....

802.11 radio information

- IEEE 802.11 Request-to-send, Flags:
- Type/Subtype: Request-to-send (0x001b)
- Frame Control Field: 0xb400
 - Version: 0
 - Type: Control frame (1)
 - Subtype: 11
 - Flags: 0x00
 - DS status: Not leaving DS or network is operating in AD-HOC mode (To DS: 0 From DS: 0) (0x0)
 - More Fragments: This is the last fragment
 - Retry: Frame is not being retransmitted
 - PWR MGT: STA will stay up
 - More Data: No data buffered
 - Protected flag: Data is not protected
 - HTC/Order Flag: Not strictly ordered
- Duration: 256 microseconds
- Receiver address: AsiarF_46:8d:49 (00:0A:52:46:8D:49)
- Transmitter address: Chongqin_9d:47:a3 (a8:93:4a:9d:47:a3)

Power management status (wlan.fc.pwrmgmt), 1 byte

Packets: 7157 · Displayed: 1676 (23.4%) Profile: Default

At frame 996, the TCP traffic has quiesced for a bit, and STA goes back to sleep.

power-save-mtk7921k-sta-mtk7915-lanforge-vap-unicast-upload.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

wlan_addr == a8:93:4a:9d:47:a3 | wlan_sa == 00:0A:52:46:8D:49

No.	Time	Source	Destination	Protocol	Length	Data rate	PHY type	Sequence number	Info
960	8.593206012	Chongqin_9d:47:a3 (- AsiarF_46:8d:49)	AsiarF_46:8d:49 (00:0A:52:46:8D:49)	802.11	76		24 802.11a (OFDM)		Request-to-send, Flags=.....
961	8.593207211	Chongqin_9d:47:a3 (- AsiarF_46:8d:49)	Chongqin_9d:47:a3 (- AsiarF_46:8d:49)	802.11	70		24 802.11a (OFDM)		Clear-to-send, Flags=.....
962	8.593374731	172.16.223.154	172.16.223.153	LANFor	1590		130 802.11n (HT)		19 Seq: 2
963	8.593376629	172.16.223.154	172.16.223.153	TCP	162		130 802.11n (HT)		20 33033 - 33034 [PSH, ACK] Seq=2909 Ack=1 Win=42 L
964	8.593377673	AsiarF_46:8d:49 (00:0A:52:46:8D:49)	Chongqin_9d:47:a3 (- AsiarF_46:8d:49)	802.11	88		24 802.11a (OFDM)		802.11 Block Ack, Flags=.....
965	8.593995230	Chongqin_9d:47:a3 (- AsiarF_46:8d:49)	Chongqin_9d:47:a3 (- AsiarF_46:8d:49)	802.11	70		6 802.11a (OFDM)		Request-to-send, Flags=.....
966	8.593996377	Chongqin_9d:47:a3 (- AsiarF_46:8d:49)	Chongqin_9d:47:a3 (- AsiarF_46:8d:49)	802.11	70		6 802.11a (OFDM)		Clear-to-send, Flags=.....
967	8.594079845	AsiarF_46:8d:49	AsiarF_46:8d:49	802.11	86		6 802.11a (OFDM)		81 QoS Null function (No data), SN=81, FN=0, Flags=
968	8.594081377	Chongqin_9d:47:a3 (- AsiarF_46:8d:49)	Chongqin_9d:47:a3 (- AsiarF_46:8d:49)	802.11	70		6 802.11a (OFDM)		Acknowledgement, Flags=.....
969	8.594398058	172.16.223.154	172.16.223.153	TCP	150		39 802.11n (HT)		9 33034 - 33033 [ACK] Seq=1 Ack=2921 Win=41 Len=0
970	8.594399979	Chongqin_9d:47:a3 (- AsiarF_46:8d:49)	AsiarF_46:8d:49 (00:0A:52:46:8D:49)	802.11	88		6 802.11a (OFDM)		802.11 Block Ack, Flags=.....
991	8.759471762	AsiarF_46:8d:49	Broadcast	802.11	330		6 802.11a (OFDM)		2980 Beacon frame, SN=2980, FN=0, Flags=....., BI=
994	8.795917821	Chongqin_9d:47:a3 (- AsiarF_46:8d:49)	Chongqin_9d:47:a3 (- AsiarF_46:8d:49)	802.11	70		6 802.11a (OFDM)		Request-to-send, Flags=.....
995	8.795920044	Chongqin_9d:47:a3 (- AsiarF_46:8d:49)	Chongqin_9d:47:a3 (- AsiarF_46:8d:49)	802.11	70		6 802.11a (OFDM)		Clear-to-send, Flags=.....
996	8.796005715	Chongqin_9d:47:a3 (- AsiarF_46:8d:49)	AsiarF_46:8d:49 (00:0A:52:46:8D:49)	802.11	86		6 802.11a (OFDM)		82 QoS Null function (No data), SN=82, FN=0, Flags=
997	8.796006990	Chongqin_9d:47:a3 (- AsiarF_46:8d:49)	AsiarF_46:8d:49 (00:0A:52:46:8D:49)	802.11	70		6 802.11a (OFDM)		Acknowledgement, Flags=.....

802.11 radio information

- IEEE 802.11 QoS Null function (No data), Flags: ...P...T
- Type/Subtype: QoS Null function (No data) (0x002c)
- Frame Control Field: 0xc811
 - Version: 0
 - Type: Data frame (2)
 - Subtype: 12
 - Flags: 0x11
 - DS status: Frame from STA to DS via an AP (To DS: 1 From DS: 0) (0x1)
 - More Fragments: This is the last fragment
 - Retry: Frame is not being retransmitted
 - PWR MGT: STA will go to sleep
 - More Data: No data buffered
 - Protected flag: Data is not protected
 - HTC/Order Flag: Not strictly ordered
- Duration: 36 microseconds
- Receiver address: AsiarF_46:8d:49 (00:0A:52:46:8D:49)
- Transmitter address: Chongqin_9d:47:a3 (a8:93:4a:9d:47:a3)
- Destination address: AsiarF_46:8d:49 (00:0A:52:46:8D:49)

Power management status (wlan.fc.pwrmgmt), 1 byte

Packets: 7157 · Displayed: 1676 (23.4%) Profile: Default