Hewlett Packard Enterprise

HPE aruba networking

Wireless Wonders: Power Save Mode & Breaking News

Dobias van Ingen

EMEA CTO & VP Systems Engineering

March 2024

Not always good to drink many beers

app-eucentral3.central.arubanetworks.com

Ekahau Insights | Aruba Central

HPE GreenLake

aruba Central

Search or ask Aruba

Customer: Ekahau, In...

Global

Manage
- Overview
- Devices
- Clients
- Guests
- Applications
- Security
- Network Services

Analyze
- Alerts & Events
- Audit Trail
- Tools
- Reports

Maintain
- Firmware
- Organization

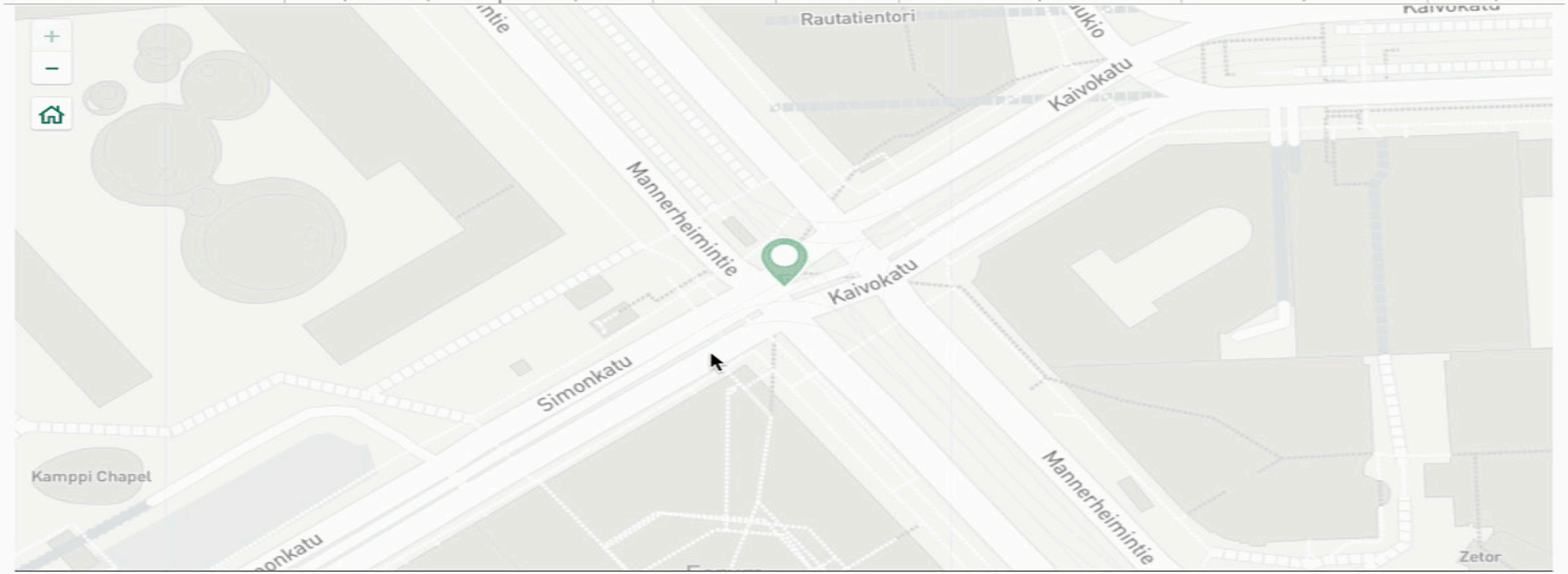
Network Health | WAN Health | Summary | Wi-Fi Connectivity | AI Insights

Summary | List

NO ISSUES | POTENTIAL ISSUES

Number of devices

Site Name	AI Insights			Status		High Mem Usage	High CPU Usage	High CH utilization		Clients		High Noise	
	HIGH	MEDIUM	LOW	UP	DOWN			2.4 GHz	5 GHz	CONNECTED	FAILED	2.4 GHz	5 GHz



1 Plotted Site(s)

Privacy | Terms of Use | Ad Choices & Cookies | Do Not Sell or Share My Personal Information

NULL DATA POWER SAVE

LEGACY POWER SAVE

TARGET WAKE TIME

VHT TXOP POWER SAVE

WMM POWER SAVE U-APSD

POWER SAVE MULTI POLL

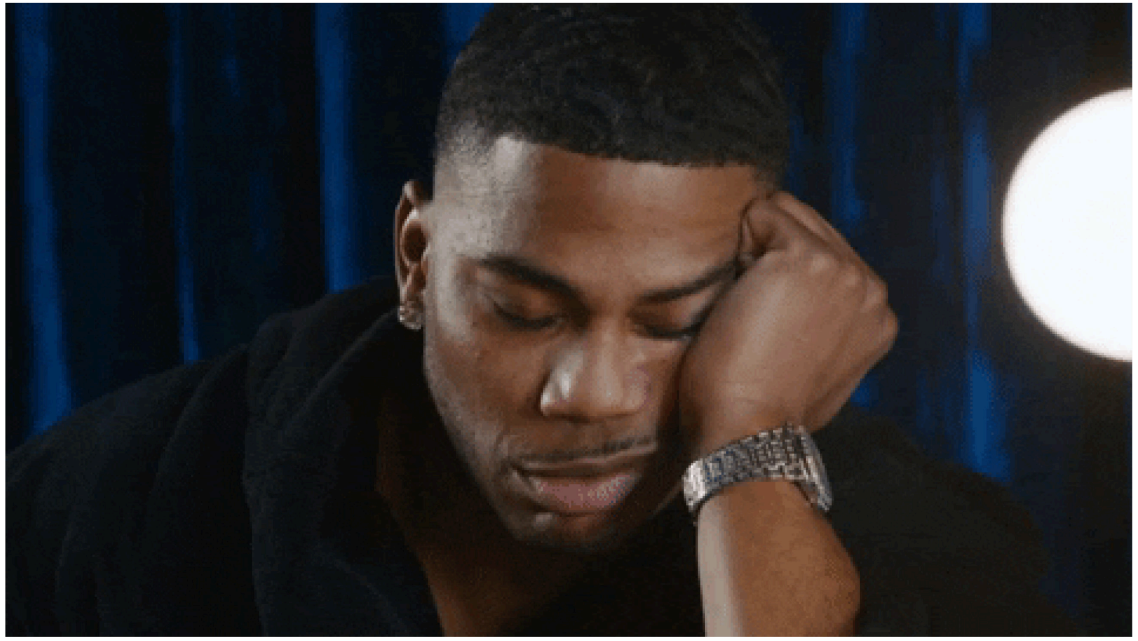
WMM POWER SAVE U-APSD

SPATIAL MULTIPLEXING POWER SAVE

Station (radio) power states

AWAKE

DOZE



Client power management modes

POWER CONSUMPTION STATES

1) Tx: Active transmission of frames
2) Rx: Receiving frames
3) Listening: Searching for frames (PHY preambles)
4) Sleep: Cannot Tx or Rx; this is the lowest power consumption state

POWER SAVE (PS)

1) In PS: Client has notified AP that of switching to PS state. This is where the AP buffers unicast frames for the client and obtains the clients permission before transmitting any unicast frames to the client.
2) Out of PS: AP can transmit unicast frames to client at any time.

Legacy PSPoll power modes

Buffer Packets

ACK

ACK

DATA
(PowerMgmt = 1)

DATA
(PowerMgmt = 0)

ACTIVE

POWER SAVE

ACTIVE

How to see AP's associations?

```
5i_work_655# sh ap association

The phy column shows client's operational capabilities for current association

Flags: H: Hotspot(802.11u) client, K: 802.11K client, M: Mu beam formee, R: 802.11R client, W: WMM client, w: 802.11w client, V: 802.11v BSS trans capable, P: Punctured preamble, U: HE UL Mu-mimo, O: OWE
C: Cellular Data Capable - network available, c: Cellular Data Capable - network unavailable, T: Individual TWT client, t: Broadcast TWT client

PHY Details: HT   : High throughput;      20: 20MHz;  40: 40MHz; t: turbo-rates (256-QAM)
             VHT  : Very High throughput; 80: 80MHz; 160: 160MHz; 80p80: 80MHz + 80MHz
             HE   : High Efficiency;       80: 80MHz; 160: 160MHz; 80p80: 80MHz + 80MHz
             <n>ss: <n> spatial streams

Association Table
-----------------
Name         bssid              mac                auth  assoc  aid  l-int  essid    vlan-id  phy_cap              phy                assoc. time     num assoc  Flags     DataReady  UAC
----         -----              ---                ----  -----  ---  -----  -----    -------  -------              ---                -----------     ---------  -----     ---------  ---
5i_work_655  34:8a:12:f8:21:93  aa:ef:49:d4:08:18  y     y      1    20     5i_Corp  30       5GHz-HE-160-2ss-RKVM 5GHz-HE-40-2ss     1h:15m:1s       1          WVKRMHhT  Yes        192.168.10.254
5i_work_655  34:8a:12:f8:21:93  88:66:5a:43:79:32  y     y      2    10     5i_Corp  30       5GHz-VHT-80sgi-3ss   5GHz-VHT-40sgi-3ss 1h:18m:37s      1          WH        Yes        192.168.10.254
5i_work_655  34:8a:12:f8:21:72  28:56:5a:55:a3:6b  y     y      1    10     5i_IoT   40       2.4GHz-HT-20sgi-1ss  2.4GHz-HT-20sgi-1ss 2h:37m:4s       1          W         Yes        192.168.10.254
Num Clients:5
```

How to verify Association ID?

```
[5i_work_655# sh ap debug client-table

Client Table
------------
MAC               ESSID    BSSID             Assoc_State  HT_State  AID  PS_State    UAPSD           TWT    Tx_Pkts  Rx_Pkts  PS_Qlen  Tx_Retries  Tx_Rate  Rx_Rate  Last_ACK_SNR  Last_Rx_SNR  TX_Chains
Idle time  Client health (C/R)  Tx_Bytes   Rx_Bytes
---               -----    -----             -----------  --------  ---  --------    -----           ---    -------  -------  -------  ----------  -------  -------  ------------  -----------  ---------
---------  ------------------  --------   --------
14:d4:24:61:3c:75  5i_IoT   34:8a:12:f8:21:92  Associated   AWvSsEBb  0x2  Power-save  (0,0,0,0,N/A,0)  (0,0)  96031    189811   0        15442       275      309      10            16           2[0x3]
900416     100/98              96102893   15100374
44:ef:bf:66:0a:7a  5i_IoT   34:8a:12:f8:21:92  Associated   WSsbB     0x1  Awake       (0,0,0,0,N/A,0)  (0,0)  2616     6818     0        1275        180      216      13            19           2[0x3]
900401     100/98              399334     1295946
88:66:5a:43:79:32  5i_Corp  34:8a:12:f8:21:93  Associated   AWvSsEe   0x2  Awake       (0,0,0,0,N/A,0)  (0,0)  715697   527172   0        10193       400      400      19            27           2[0x3]
900400     100/98              [illegible]  411780071
aa:ef:49:d4:08:18  5i_Corp  34:8a:12:f8:21:93  Associated   AWvSsE    0x1  Power-save  (0,0,0,0,N/A,0)  (0,0)  34       206      0        11          344      195      18            28           2[0x3]
900408     100/98              10806      8853
28:56:5a:55:a3:6b  5i_IoT   34:8a:12:f8:21:72  Associated   Qs        0x1  Awake       (0,0,0,0,N/A,0)  (0,0)  207      616      0        70          72       72       56            45           1[0x1]
900402     100/100             14216      34798
```

Verify more detailed info per client?

```
[5i_work_655# sh client status aa:ef:49:d4:08:18

 STA Table
 ---------
bssid              auth  assoc  aid  l-int  essid    vlan-id  tunnel-id  name    ip-ready  authenticated  CP returned radius ip  device type string  Acct-Authentic
-----              ----  -----  ---  -----  -----    -------  ---------  ----    --------  -------------  ----------------------  ------------------  --------------
34:8a:12:f8:21:93  y     y      1    20     5i_Corp  30       0x0        dingen  y         y              0.0.0.0                 NOFP                1
STA Table(continues)
--------------------
acct-status  acct-sessid                              cached-inocts  cached-outocts  cached-inpkts  cached-outpkts  cached-sesstim  Start time
-----------  -----------                              -------------  --------------  -------------  --------------  --------------  ----------
3            348A12F82193-AAEF49D40818-65980459-45C21  0              0               0              0               0               3286
State Hash Table
----------------
bssid              state       reason
-----              -----       ------
34:8a:12:f8:21:93  auth-assoc  0
Rap Bridge User Table
---------------------
action  ip            mac                aclnum  bssid              essid    vlanid  wired
------  --            ---                ------  -----              -----    ------  -----
0       192.168.30.8  aa:ef:49:d4:08:18  154     34:8a:12:f8:21:93  5i_Corp  30      0
State Summary Table  (apstm:0x626 anul:0x626 host:0x616 enc:0x40)
-----------------------------------------------------------------
Module  IV  A1  A2  AF  Alg  A3  A4  AsQ  AsR  Drv  AsF  IDQ  IDR  TxID  RxID  Start  Succ  TxEF  RxEF  KTx  KRx
------  --  --  --  --  ---  --  --  ---  ---  ---  ---  ---  ---  ----  ----  -----  ----  ----  ----  ---  ---
APSTM   0   1   1   0   2    0   0   1    1    0    0    0    0    0     0     0      0     0     0     0    0
ANUL    0   1   1   0   2    0   0   1    1    0    0    0    0    0     0     0      0     0     0     0    0
Host    0   1   1   0   0    0   0   1    1    0    0    0    0    0     0     0      0     0     0     0    0

Analysis: dot1x-no-eapid-req-tx dot1x-no-eapid-resp-rx dot1x-no-success 4way-incomplete dot1x-no-eap-start-rx


Key:
IV:invalid if set. A1-A4 is Auth 1-4 and AF is Auth-Fail. A1-2 are for Auth-Req/Resp.
    SAE uses A3/4 for Confirm request/response. Only host processes A2 unless SAE/FT
Alg: represents authentication algorithm. 0:Open, 1:Shared, 2:11r-FT, 3:SAE
AsQ:assoc-req, AsR:assoc-resp, Drv:driver-assoc-turnaround (if set only host shows response), AsF:assoc-fail
EAPOL - IDQ:EAP-ID-req, IDR:EAP-ID-resp, TxID:Last-TX-EapID, RxID:Last-RX-EapID, Start:Start
        Succ:Success, TxEF:EAP-Fail-TX, RxEF:EAP-Fail-RX, KTx:TX-key-count, KRx:RX-key-count
```

MAC addr STA

Association identifier

Per bssid, per client

AID in packet captures?

247	7.31…	aa:ef:49:d4:08:18	ArubaaHe_f8:21:93	802.11	320	STA will stay up	Association Request, SN=2249, FN=0, Flags=........C,
248	7.31…		aa:ef:49:d4:08:18 (aa:ef:49:d4:08:18) (RA)	802.11	68	STA will stay up	Acknowledgement, Flags=........C
249	7.31…	ArubaaHe_f8:21:93	aa:ef:49:d4:08:18	802.11	377	STA will stay up	Association Response, SN=1, FN=0, Flags=........C
250	7.31…		ArubaaHe_f8:21:93 (34:8a:12:f8:21:93) (RA)	802.11	68	STA will stay up	Acknowledgement, Flags=........C

```
> Frame 249: 377 bytes on wire (3016 bits), 377 bytes captured (3016 bits) on interface en0, id 0
> Radiotap Header v0, Length 56
> 802.11 radio information
v IEEE 802.11 Association Response, Flags: ........C
    Type/Subtype: Association Response (0x0001)
  v Frame Control Field: 0x1000
      .... ..00 = Version: 0
      .... 00.. = Type: Management frame (0)
      0001 .... = Subtype: 1
    v Flags: 0x00
        .... ..00 = DS status: Not leaving DS or network is operating in AD-HOC mode (To DS: 0 From DS: 0) (0x0)
        .... .0.. = More Fragments: This is the last fragment
        .... 0... = Retry: Frame is not being retransmitted
        ...0 .... = PWR MGT: STA will stay up
        ..0. .... = More Data: No data buffered
        .0.. .... = Protected flag: Data is not protected
        0... .... = +HTC/Order flag: Not strictly ordered
    .000 0000 0011 1100 = Duration: 60 microseconds
    Receiver address: aa:ef:49:d4:08:18 (aa:ef:49:d4:08:18)
    Destination address: aa:ef:49:d4:08:18 (aa:ef:49:d4:08:18)
    Transmitter address: ArubaaHe_f8:21:93 (34:8a:12:f8:21:93)
    Source address: ArubaaHe_f8:21:93 (34:8a:12:f8:21:93)
    BSS Id: ArubaaHe_f8:21:93 (34:8a:12:f8:21:93)
    .... .... .... 0000 = Fragment number: 0
    0000 0000 0001 .... = Sequence number: 1
    Frame check sequence: 0xd12697e7 [unverified]
    [FCS Status: Unverified]
v IEEE 802.11 Wireless Management
  v Fixed parameters (6 bytes)
    > Capabilities Information: 0x1011
      Status code: Successful (0x0000)
      ..00 0000 0000 0001 = Association ID: 0x0001
  v Tagged parameters (257 bytes)
    > Tag: Supported Rates 6(B), 9, 12(B), 18, 24(B), 36, 48, 54, [Mbit/sec]
    > Tag: RM Enabled Capabilities (5 octets)
    > Tag: Mobility Domain
    > Tag: Fast BSS Transition
    > Tag: HT Capabilities (802.11n D1.10)
    > Tag: HT Information (802.11n D1.10)
    > Tag: Extended Capabilities (8 octets)
    > Tag: VHT Capabilities
    > Tag: VHT Operation
    > Ext Tag: HE Capabilities
    > Ext Tag: HE Operation
    > Ext Tag: MU EDCA Parameter Set
    > Tag: Vendor Specific: Microsoft Corp.: WMM/WME: Parameter Element
```

Station notifies AP to buffer packets

```
344 7.84…  aa:ef:49:d4:08:18   ArubaaHe_f8:21:93          802.11   84   STA will go to sleep   Null function (No data), SN=2258, FN=0, Flags=...P...TC
345 7.84…                      aa:ef:49:d4:08:18 (aa:ef:49:… 802.11   68   STA will stay up       Acknowledgement, Flags=........C
```

AP ‘ACKs’ the message

```
> Frame 344: 84 bytes on wire (672 bits), 84 bytes captured (672 bits) on interface en0, id 0
> Radiotap Header v0, Length 56
> 802.11 radio information
v IEEE 802.11 Null function (No data), Flags: ...P...TC
    Type/Subtype: Null function (No data) (0x0024)
  v Frame Control Field: 0x4811
      .... ..00 = Version: 0
      .... 10.. = Type: Data frame (2)
      0100 .... = Subtype: 4
    v 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... .... = +HTC/Order flag: Not strictly ordered
    .000 0000 0010 1100 = Duration: 44 microseconds
    Receiver address: ArubaaHe_f8:21:93 (34:8a:12:f8:21:93)
    Transmitter address: aa:ef:49:d4:08:18 (aa:ef:49:d4:08:18)
    Destination address: ArubaaHe_f8:21:93 (34:8a:12:f8:21:93)
    Source address: aa:ef:49:d4:08:18 (aa:ef:49:d4:08:18)
    BSS Id: ArubaaHe_f8:21:93 (34:8a:12:f8:21:93)
    STA address: aa:ef:49:d4:08:18 (aa:ef:49:d4:08:18)
    .... .... .... 0000 = Fragment number: 0
    1000 1101 0010 .... = Sequence number: 2258
    Frame check sequence: 0xbb88923e [unverified]
    [FCS Status: Unverified]
```

Station becomes active

2.45…	ArubaaHe_f8:21:93	Broadcast	802.11	477	0x01	STA will stay up	Beacon frame, SN=1333, FN=0, Flags=........C, BI=100, SSID="5i_Corp"
2.45…	aa:ef:49:d4:08:18	ArubaaHe_f8:21:93	802.11	84		STA will stay up	Null function (No data), SN=2640, FN=0, Flags=.......TC
2.45…		aa:ef:49:d4:08:18 (aa:ef:49:…	802.11	68		STA will stay up	Acknowledgement, Flags=........C
2.46…	ArubaaHe_f8:21:93 (3…	aa:ef:49:d4:08:18 (aa:ef:49:…	802.11	113		STA will stay up	Trigger Buffer Status Report Poll (BSRP), Flags=........C
2.52…	aa:ef:49:d4:08:18	ArubaaHe_f8:21:93	802.11	84		STA will go to sleep	Null function (No data), SN=2641, FN=0, Flags=...P...TC

```
> Frame 92: 477 bytes on wire (3816 bits), 477 bytes captured (3816 bits) on interface en0, id 0
> Radiotap Header v0, Length 56
> 802.11 radio information
> IEEE 802.11 Beacon frame, Flags: ........C
v IEEE 802.11 Wireless Management
  v Fixed parameters (12 bytes)
      Timestamp: 1474217472515
      Beacon Interval: 0.102400 [Seconds]
    > Capabilities Information: 0x1411
  v Tagged parameters (381 bytes)
    > Tag: SSID parameter set: "5i_Corp"
    > Tag: Supported Rates 6(B), 9, 12(B), 18, 24(B), 36, 48, 54, [Mbit/sec]
    > Tag: DS Parameter set: Current Channel: 161
    v Tag: Traffic Indication Map (TIM): DTIM 0 of 1 bitmap
        Tag Number: Traffic Indication Map (TIM) (5)
        Tag length: 4
        DTIM count: 0
        DTIM period: 1
      > Bitmap control: 0x00
        Partial Virtual Bitmap: 02
        Association ID: 0x01
```

```
> Frame 94: 84 bytes on wire (672 bits), 84 bytes captured (672 bits) on interface en0, id 0
> Radiotap Header v0, Length 56
> 802.11 radio information
v IEEE 802.11 Null function (No data), Flags: .......TC
    Type/Subtype: Null function (No data) (0x0024)
  v Frame Control Field: 0x4801
      .... ..00 = Version: 0
      .... 10.. = Type: Data frame (2)
      0100 .... = Subtype: 4
    v Flags: 0x01
        .... ..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 .... = PWR MGT: STA will stay up
        ..0. .... = More Data: No data buffered
        .0.. .... = Protected flag: Data is not protected
        0... .... = +HTC/Order flag: Not strictly ordered
    .000 0000 0010 1100 = Duration: 44 microseconds
    Receiver address: ArubaaHe_f8:21:93 (34:8a:12:f8:21:93)
    Transmitter address: aa:ef:49:d4:08:18 (aa:ef:49:d4:08:18)
    Destination address: ArubaaHe_f8:21:93 (34:8a:12:f8:21:93)
    Source address: aa:ef:49:d4:08:18 (aa:ef:49:d4:08:18)
    BSS Id: ArubaaHe_f8:21:93 (34:8a:12:f8:21:93)
    STA address: aa:ef:49:d4:08:18 (aa:ef:49:d4:08:18)
    .... .... .... 0000 = Fragment number: 0
    1010 0101 0000 .... = Sequence number: 2640
    Frame check sequence: 0x1acb982a [unverified]
    [FCS Status: Unverified]
```

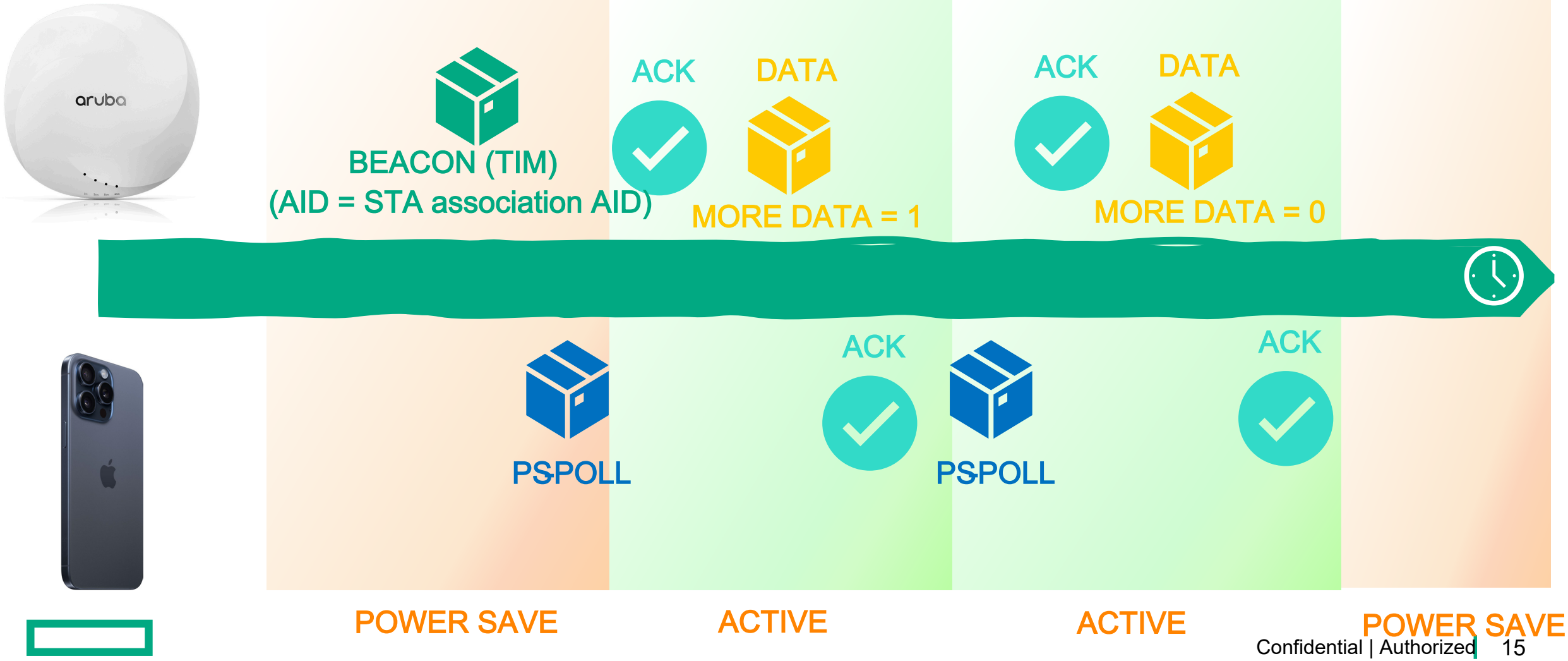
For how long AP needs to buffer?

```
> Frame 247: 320 bytes on wire (2560 bits), 320 bytes captured (2560 bits) on interface en0, id 0
> Radiotap Header v0, Length 56
> 802.11 radio information
v IEEE 802.11 Association Request, Flags: ........C
    Type/Subtype: Association Request (0x0000)
  > Frame Control Field: 0x0000
```

```
> Frame 315: 199 bytes on wire (1592 bits), 199 bytes captured (1592 bits) on interface en0, id 0
> Radiotap Header v0, Length 56
> 802.11 radio information
v IEEE 802.11 Association Request, Flags: ........C
    Type/Subtype: Association Request (0x0000)
  > Frame Control Field: 0x0000
    .000 0000 0011 1010 = Duration: 58 microseconds
    Receiver address: HewlettP_1a:e0:f3 (9c:8c:d8:1a:e0:f3)
    Destination address: HewlettP_1a:e0:f3 (9c:8c:d8:1a:e0:f3)
    Transmitter address: AzureWav_07:36:db (50:5a:65:07:36:db)
    Source address: AzureWav_07:36:db (50:5a:65:07:36:db)
    BSS Id: HewlettP_1a:e0:f3 (9c:8c:d8:1a:e0:f3)
    .... .... .... 0000 = Fragment number: 0
    0000 0000 0001 .... = Sequence number: 1
    Frame check sequence: 0x3763751e [unverified]
    [FCS Status: Unverified]
v IEEE 802.11 Wireless Management
  v Fixed parameters (4 bytes)
    > Capabilities Information: 0x0611
      Listen Interval: 0x0001
  > Tagged parameters (111 bytes)
```

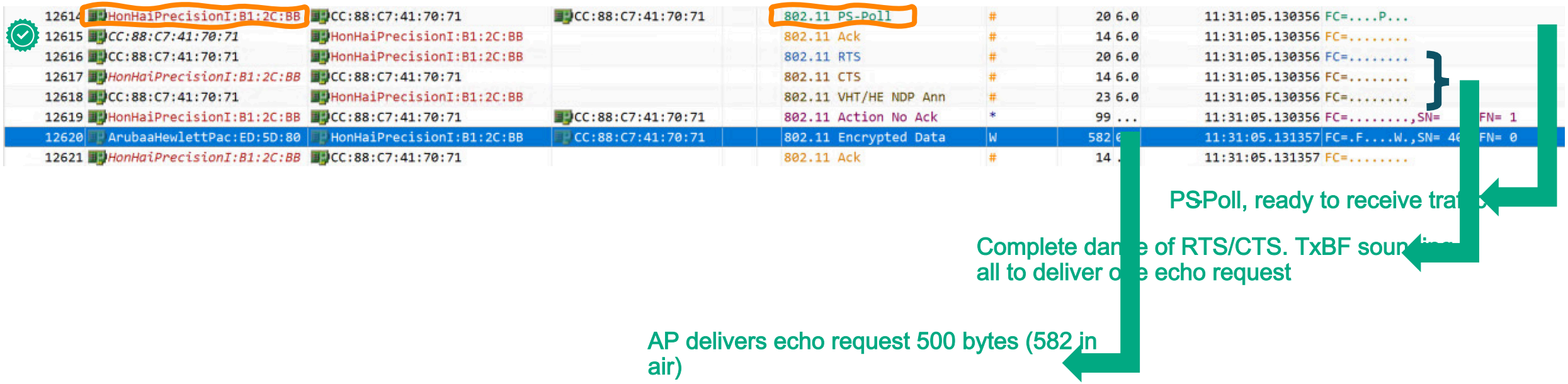
Windows laptop

Legacy PS-Poll mode buffered unicast delivery



Legacy PSPoll mode

TRAFFIC BUFFERED AT AP



Traffic Identification Map
TIM Element

```
8.09…  ArubaaHe_f8:21:93     Broadcast                802.11       477 0x01…  STA will stay up          161 Beacon frame, SN=597, FN=0, Flags=........C, BI=100, SSID="5i_Corp"
```

```
> Frame 553: 477 bytes on wire (3816 bits), 477 bytes captured (3816 bits) on interface en0, id 0
> Radiotap Header v0, Length 56
> 802.11 radio information
> IEEE 802.11 Beacon frame, Flags: ........C
v IEEE 802.11 Wireless Management
  > Fixed parameters (12 bytes)
  v Tagged parameters (381 bytes)
    > Tag: SSID parameter set: "5i_Corp"
    > Tag: Supported Rates 6(B), 9, 12(B), 18, 24(B), 36, 48, 54, [Mbit/sec]
    > Tag: DS Parameter set: Current Channel: 161
    v Tag: Traffic Indication Map (TIM): DTIM 0 of 1 bitmap
        Tag Number: Traffic Indication Map (TIM) (5)
        Tag length: 4
        DTIM count: 0
        DTIM period: 1
      v Bitmap control: 0x00
          .... ...0 = Multicast: False
          0000 000. = Bitmap Offset: 0x00
        Partial Virtual Bitmap: 02
        Association ID: 0x01
```

Traffic buffered for AID

DTIM (1)

```
> Frame 414: 477 bytes on wire (3816 bits), 477 bytes captured (3816 bits) on interface en0, id 0
> Radiotap Header v0, Length 56
> 802.11 radio information
> IEEE 802.11 Beacon frame, Flags: ........C
v IEEE 802.11 Wireless Management
  > Fixed parameters (12 bytes)
  v Tagged parameters (381 bytes)
    > Tag: SSID parameter set: "5i_Corp"
    > Tag: Supported Rates 6(B), 9, 12(B), 18, 24(B), 36, 48, 54, [Mbit/sec]
    > Tag: DS Parameter set: Current Channel: 161
    v Tag: Traffic Indication Map (TIM): DTIM 0 of 1 bitmap
        Tag Number: Traffic Indication Map (TIM) (5)
        Tag length: 4
        DTIM count: 0
        DTIM period: 1
      > Bitmap control: 0x00
        Partial Virtual Bitmap: 06
        Association ID: 0x01
        Association ID: 0x02
```

Value of 0 means current TIM is DTIM

HPE Aruba default DTIM int. = 1 beacon.

Meaning all TIMs are DTIMs. (0 is reserved)

DTIM (2)

```
0.00…  ArubaaHe_f8:21:93   Broadcast   802.11   477   STA will stay up   161  Beacon frame, SN=3407, FN=0, Flags=........C, BI=100, SSID="5i_Corp
0.10…  ArubaaHe_f8:21:93   Broadcast   802.11   477   STA will stay up   161  Beacon frame, SN=3408, FN=0, Flags=........C, BI=100, SSID="5i_Corp
0.20…  ArubaaHe_f8:21:93   Broadcast   802.11   477   STA will stay up   161  Beacon frame, SN=3409, FN=0, Flags=........C, BI=100, SSID="5i_Corp
```

```
> Frame 2: 477 bytes on wire (3816 bits), 477 bytes captured (3816 bits) on interface en0, id 0
> Radiotap Header v0, Length 56
> 802.11 radio information
> IEEE 802.11 Beacon frame, Flags: ........C
v IEEE 802.11 Wireless Management
  > Fixed parameters (12 b
  v Tagged parameters (381
    > Tag: SSID parameter
    > Tag: Supported Rates
    > Tag: DS Parameter se
    v Tag: Traffic Indicat
        Tag Number: Traff
        Tag length: 4
        DTIM count: 2
        DTIM period: 3
      > Bitmap control: 0
        Partial Virtual B
```

#b

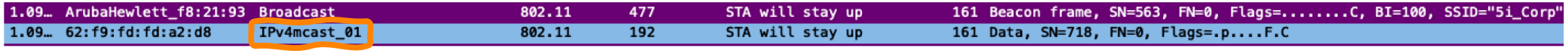
```
> Frame 5: 477 bytes on wire (3816 bits), 477 bytes captured (3816 bits) on interface en0, id 0
> Radiotap Header v0, Length 56
> 802.11 radio information
> IEEE 802.11 Beacon frame, Flags: ........C
v IEEE 802.11 Wireless Management
  > Fixed parameters (12 bytes)
  v Tagged parameters (381 bytes)
    > Tag: SSID parameter
    > Tag: Supported Rate
    > Tag: DS Parameter s
    v Tag: Traffic Indica
        Tag Number: Traf
        Tag length: 4
        DTIM count: 1
        DTIM period: 3
      > Bitmap control: (
        Partial Virtual I
```

```
> Frame 8: 477 bytes on wire (3816 bits), 477 bytes captured (3816 bits) on interface en0, id 0
> Radiotap Header v0, Length 56
> 802.11 radio information
> IEEE 802.11 Beacon frame, Flags: ........C
v IEEE 802.11 Wireless Management
  > Fixed parameters (12 bytes)
  v Tagged parameters (381 bytes)
    > Tag: SSID parameter set: "5i_Corp"
    > Tag: Supported Rates 6(B), 9, 12(B), 18, 24(B), 36, 48, 54, [Mbit/sec]
    > Tag: DS Parameter set: Current Channel: 161
    v Tag: Traffic Indication Map (TIM): DTIM 0 of 3 bitmap
        Tag Number: Traffic Indication Map (TIM) (5)
        Tag length: 4
        DTIM count: 0
        DTIM period: 3
      > Bitmap control: 0x00
        Partial Virtual Bitmap: 00
```

= current TIM is DTIM

DTIM (3)
Broadcast / Multicast

Data directly send by AP after DTIM




```
> Frame 338: 477 bytes on wire (3816 bits), 477 bytes captured (3816 bits) on interface en0, id 0
> Radiotap Header v0, Length 56
> 802.11 radio information
> IEEE 802.11 Beacon frame, Flags: ........C
v IEEE 802.11 Wireless Management
  > Fixed parameters (12 bytes)
  v Tagged parameters (381 bytes)
    > Tag: SSID parameter set: "5i_Corp"
    > Tag: Supported Rates 6(B), 9, 12(B), 18, 24(B), 36, 48, 54, [Mbit/sec]
    > Tag: DS Parameter set: Current Channel: 161
    v Tag: Traffic Indication Map (TIM): DTIM 0 of 1 bitmap
        Tag Number: Traffic Indication Map (TIM) (5)
        Tag length: 4
        DTIM count: 0
        DTIM period: 1
      v Bitmap control: 0x01
          .... ...1 = Multicast: True
          0000 000. = Bitmap Offset: 0x00
        Partial Virtual Bitmap: 04
        Association ID: 0x02
```

First bit = 1, broadcast or multicast traffic is buffered at AP

Yes, as ancient as it might sound

But. …

- Many organizations use ancient handhelds
  - Healthcare / Retail markets
- Still VHT devices that exercise PS-Poll for traffic delivery

CAN’T THIS BE DONE MORE OPTIMIZED

LET’S LOOK AT POPULAR METHOD

De-facto solution in industry *(Null Data Power Save)*

BEACON (TIM)
(AID = STA association AID)

ACK

DATA

MORE DATA = 1

DATA

MORE DATA = 0

ACK

NULL DATA
(PWR MGMT = 0)

ACK

ACK

NULL DATA
(PWR MGMT = 1)

POWER SAVE

ACTIVE

ACTIVE

POWER SAVE

Before jumping to next step…..
The NULL what????

- Null Data Frame is a control frame
- Only transmitted by STA
- No data payload

10	Data	0100	Null

```
Frame 1: 84 bytes on wire (672 bits), 84 bytes captured (672 bits) on interface en0, id 0
Radiotap Header v0, Length 56
802.11 radio information
IEEE 802.11 Null function (No data), Flags: ...P..TC
    Type/Subtype: Null function (No data) (0x0024)
    Frame Control Field: 0x4811
        .... ..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... .... = +HTC/Order flag: Not strictly ordered
    .000 0000 0010 1100 = Duration: 44 microseconds
    Receiver address: ArubaHewlett_f8:21:93 (34:8a:12:f8:21:93)
    Transmitter address: 62:f9:fd:fd:a2:d8 (62:f9:fd:fd:a2:d8)
    Destination address: ArubaHewlett_f8:21:93 (34:8a:12:f8:21:93)
    Source address: 62:f9:fd:fd:a2:d8 (62:f9:fd:fd:a2:d8)
    BSS Id: ArubaHewlett_f8:21:93 (34:8a:12:f8:21:93)
    STA address: 62:f9:fd:fd:a2:d8 (62:f9:fd:fd:a2:d8)
    .... .... .... 0000 = Fragment number: 0
    0100 0010 1100 .... = Sequence number: 1068
    Frame check sequence: 0x87d88b48 [unverified]
    [FCS Status: Unverified]
    [WLAN Flags: ...P...TC]
```

De-facto method
Google Pixel 6 ⇆ Macbook (ping)

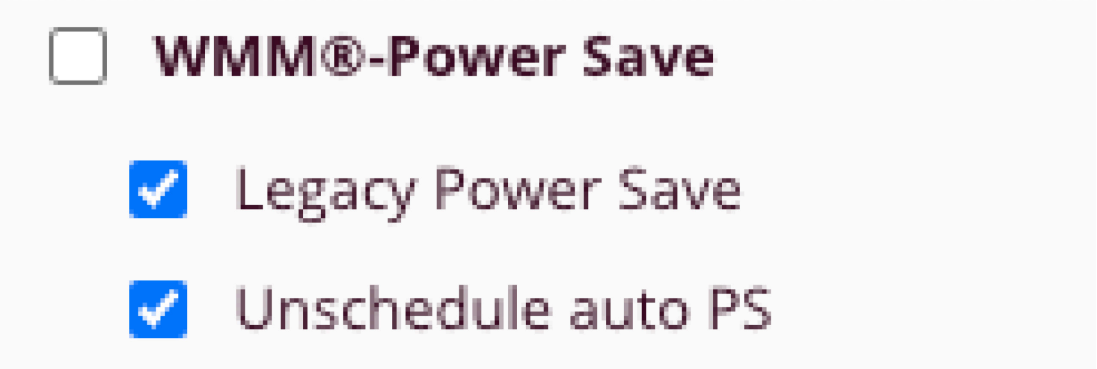
Time	Source	Destination
0.000000	192.168.40.246	192.168.40.211
0.033943	ArubaHewlett_f8:21:93	Broadcast
0.045975	b2:00:ac:34:4e:11	ArubaHewlett_f8:21:93
0.048059		b2:00:ac:34:4e:11 (b2:00:ac:3
0.048067	192.168.40.246	192.168.40.211
0.056129	b2:00:ac:34:4e:11 (b2:00:ac:34:4e:11) (TA)	ArubaHewlett_f8:21:93 (34:8a:1
0.056135		b2:00:ac:34:4e:11 (b2:00:ac:34
0.056142	b2:00:ac:34:4e:11 (b2:00:ac:34:4e:11) (TA)	ArubaHewlett_f8:21:93 (34:8a:1
0.056148		b2:00:ac:34:4e:11 (b2:00:ac:34
0.056154	b2:00:ac:34:4e:11 (b2:00:ac:34:4e:11) (TA)	ArubaHewlett_f8:21:93 (34:8a:1
0.056160		b2:00:ac:34:4e:11 (b2:00:ac:34
0.056168	192.168.40.211	192.168.40.246
0.093967	ArubaHewlett_f8:21:93 (34:8a:12:f8:21:93) (TA)	b2:00:ac:34:4e:11 (b2:00:ac:34
0.093978	b2:00:ac:34:4e:11	ArubaHewlett_f8:21:93
0.115952		b2:00:ac:34:4e:11 (b2:00:ac:34

```
> Frame 14: 76 bytes on wire (608 bits), 76 bytes captured (608 bits)
> Radiotap Header v0, Length 48
> 802.11 radio information
v IEEE 802.11 Null function (No data), Flags: ...P...TC
    Type/Subtype: Null function (No data) (0x0024)
  v Frame Control Field: 0x4811
      .... ..00 = Version: 0
      .... 10.. = Type: Data frame (2)
      0100 .... = Subtype: 4
    v 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... .... = +HTC/Order flag: Not strictly ordered
    ...00 0000 0011 1100 = Duration: 60 microseconds
    Receiver address: ArubaHewlett_f8:21:93 (34:8a:12:f8:21:93)
    Transmitter address: b2:00:ac:34:4e:11 (b2:00:ac:34:4e:11)
    Destination address: ArubaHewlett_f8:21:93 (34:8a:12:f8:21:93)
    Source address: b2:00:ac:34:4e:11 (b2:00:ac:34:4e:11)
    BSS Id: ArubaHewlett_f8:21:93 (34:8a:12:f8:21:93)
    STA address: b2:00:ac:34:4e:11 (b2:00:ac:34:4e:11)
    .... .... .... 0000 = Fragment number: 0
    0101 1011 0101 .... = Sequence number: 1461
    Frame check sequence: 0x46f6c8ad [unverified]
    [FCS Status: Unverified]
    [WLAN Flags: ...P...TC]
```

```
    DTIM count: 0
    DTIM period: 1
  > Bitmap control: 0x00
    Partial Virtual Bitmap: 04
    Association ID: 0x0002
```

Automatic Power Save Delivery (APSD)

- Introduced in IEEE 802.11e amendment - 2005
  - Became part of IEEE 802.11-2020 standard
  - Backward compatible with legacy PS delivery
- WMM-PS enhancement over legacy power saving
- Goal of WMM-PS:
  - Client device more in sleep state
  - Minimize latency for time-sensitive applications
- Two APSD methods defined:
  - Scheduled APSD (S-APSD)
  - Unscheduled APSD (U-APSD)

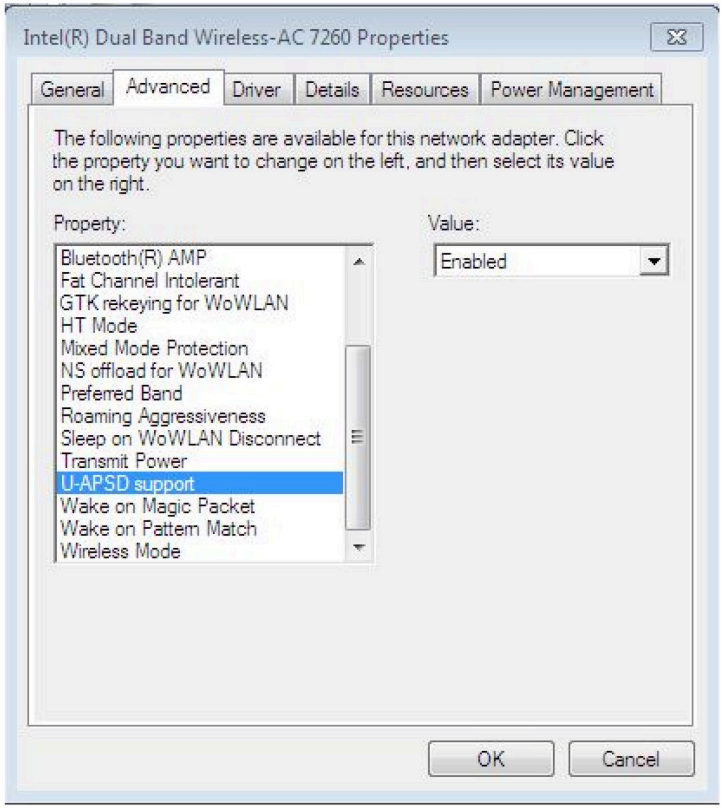


Intel

U-APSD support

U-APSD (or WMM-Power Save or WMM-PS) is a Wi-Fi capability that saves power consumption on low periodic latency-sensitive traffic modes, like a VoIP. We have identified interoperability (IOT) issues with certain access points that result in reduced RX throughput.

- **Enabled**
- **Disabled (default)**



https://www.intel.com/content/www/us/en/support/articles/000005585/wireless/legacy-intel-wireless-products.html

WMM UAPSD

ACK

QOS DATA
(EOSP = 0)

QOS DATA
(EOSP = 1)

QOS DATA
(Trigger AC)

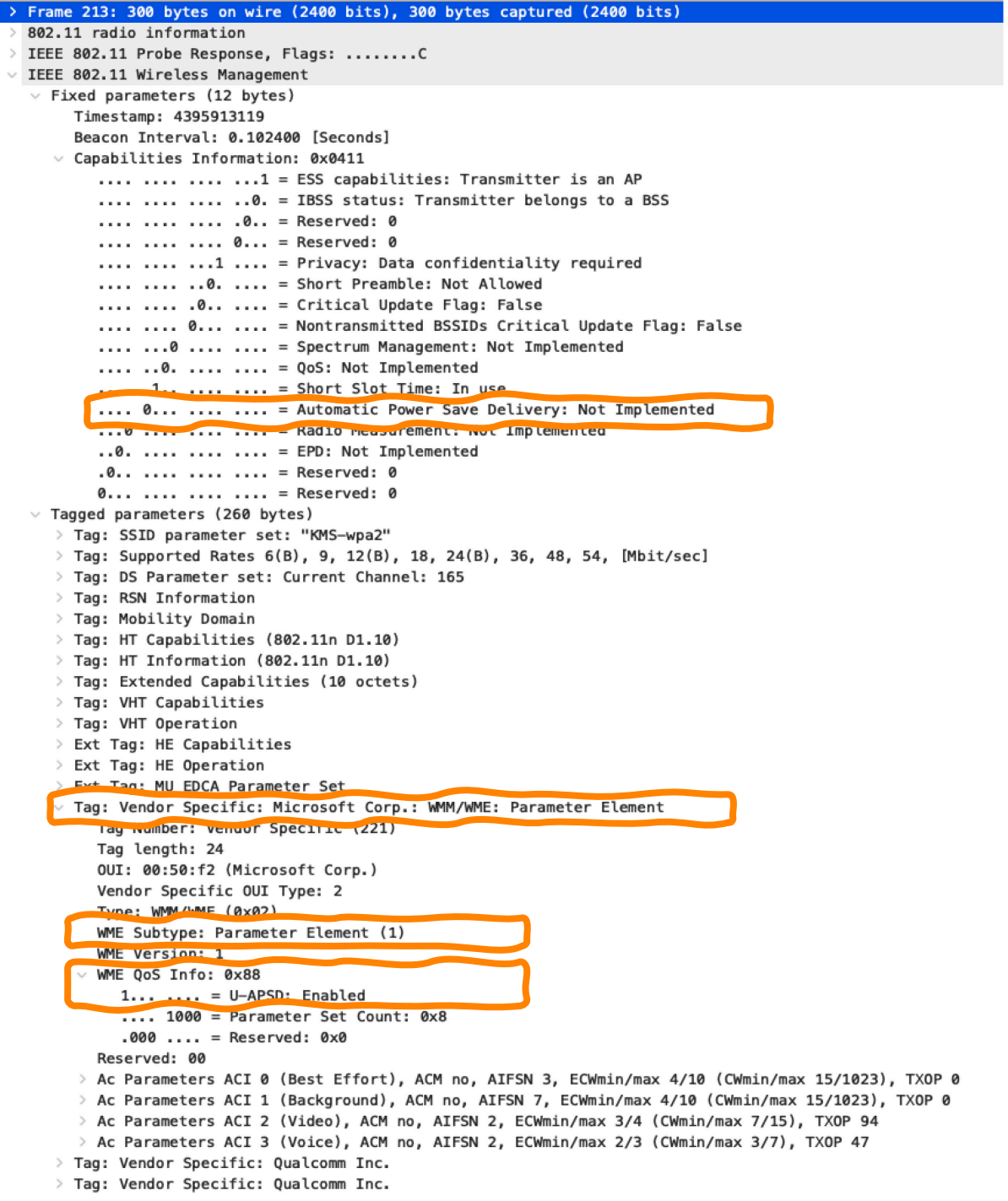
ACK

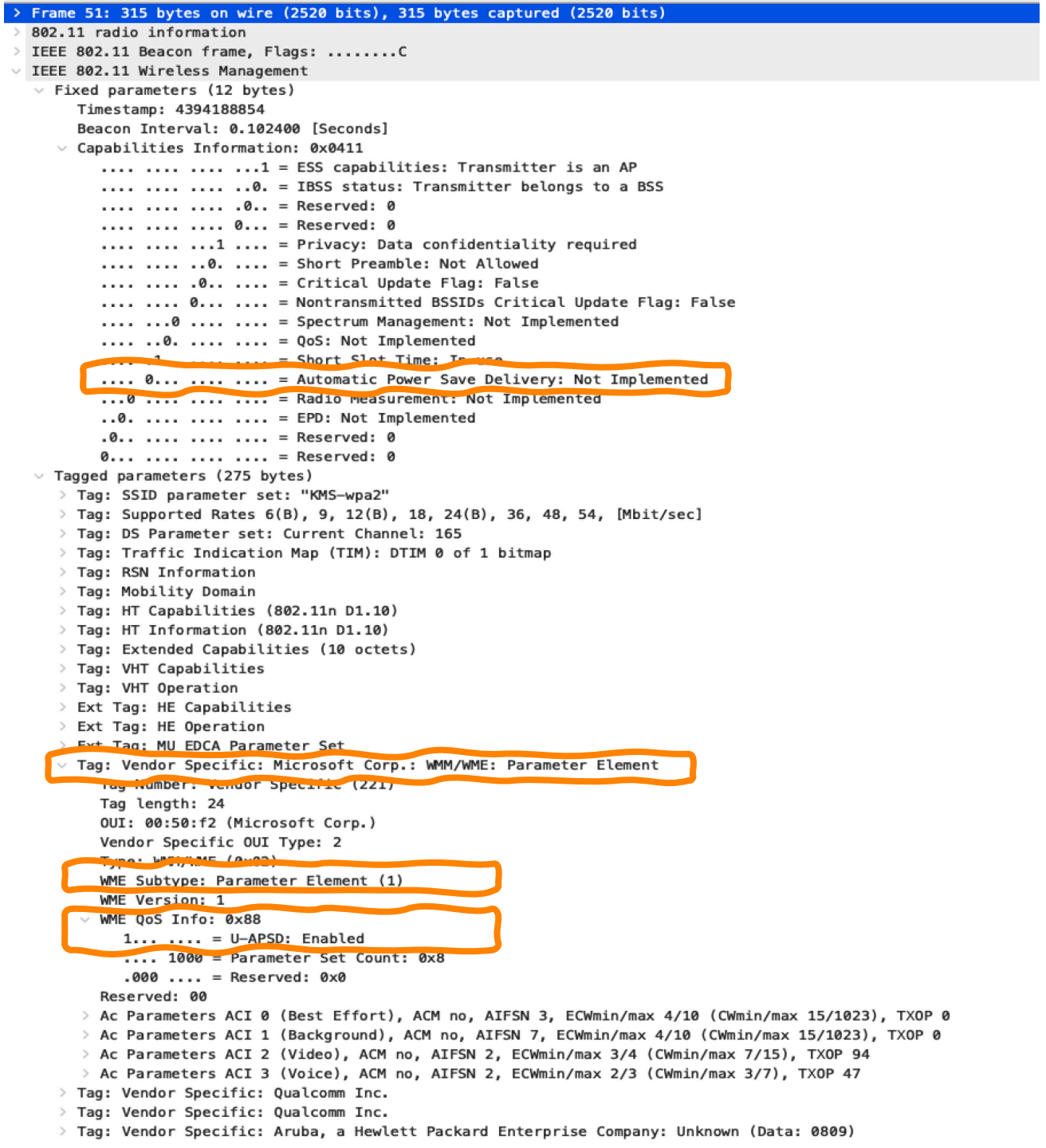
ACK

POWER SAVE

ACTIVE

POWER SAVE


Frame 213: 300 bytes on wire (2400 bits), 300 bytes captured (2400 bits)
802.11 radio information
IEEE 802.11 Probe Response, Flags: C
IEEE 802.11 Wireless Management
Fixed parameters (12 bytes)
Timestamp: 4395913119
Beacon Interval: 0.102400 [Seconds]
Capabilities Information: 0x0411
....1 = ESS capabilities: Transmitter is an AP
....0. = IBSS status: Transmitter belongs to a BSS
.... .0.. = Reserved: 0
.... 0... = Reserved: 0
....1 .... = Privacy: Data confidentiality required
....0. .... = Short Preamble: Not Allowed
.... .0.. .... = Critical Update Flag: False
.... 0... .... = Nontransmitted BSSIDs Critical Update Flag: False
....0 .... = Spectrum Management: Not Implemented
.... ..0. .... = QoS: Not Implemented
.... 1... .... = Short Slot Time: In use
.... 0... .... = Automatic Power Save Delivery: Not Implemented
...0 .... = Radio Measurement: Not Implemented
..0. .... = EPD: Not Implemented
.0.. .... = Reserved: 0
0... .... = Reserved: 0
Tagged parameters (260 bytes)
Tag: SSID parameter set: "KMS-wpa2"
Tag: Supported Rates 6(B), 9, 12(B), 18, 24(B), 36, 48, 54, [Mbit/sec]
Tag: DS Parameter set: Current Channel: 165
Tag: RSN Information
Tag: Mobility Domain
Tag: HT Capabilities (802.11n D1.10)
Tag: HT Information (802.11n D1.10)
Tag: Extended Capabilities (10 octets)
Tag: VHT Capabilities
Tag: VHT Operation
Ext Tag: HE Capabilities
Ext Tag: HE Operation
Ext Tag: MU EDCA Parameter Set
Tag: Vendor Specific: Microsoft Corp.: WMM/WME: Parameter Element
Tag Number: Vendor Specific (221)
Tag length: 24
OUI: 00:50:f2 (Microsoft Corp.)
Vendor Specific OUI Type: 2
Type: WMM/WME (0x02)
WME Subtype: Parameter Element (1)
WME Version: 1
WME QoS Info: 0x88
1... .... = U-APSD: Enabled
.... 1000 = Parameter Set Count: 0x8
.000 .... = Reserved: 0x0
Reserved: 00
Ac Parameters ACI 0 (Best Effort), ACM no, AIFSN 3, ECWmin/max 4/10 (CWmin/max 15/1023), TXOP 0
Ac Parameters ACI 1 (Background), ACM no, AIFSN 7, ECWmin/max 4/10 (CWmin/max 15/1023), TXOP 0
Ac Parameters ACI 2 (Video), ACM no, AIFSN 2, ECWmin/max 3/4 (CWmin/max 7/15), TXOP 94
Ac Parameters ACI 3 (Voice), ACM no, AIFSN 2, ECWmin/max 2/3 (CWmin/max 3/7), TXOP 47
Tag: Vendor Specific: Qualcomm Inc.
Tag: Vendor Specific: Qualcomm Inc.


Frame 51: 315 bytes on wire (2520 bits), 315 bytes captured (2520 bits)
802.11 radio information
IEEE 802.11 Beacon frame, Flags: C
IEEE 802.11 Wireless Management
Fixed parameters (12 bytes)
Timestamp: 4394188854
Beacon Interval: 0.102400 [Seconds]
Capabilities Information: 0x0411
....1 = ESS capabilities: Transmitter is an AP
....0. = IBSS status: Transmitter belongs to a BSS
.... .0.. = Reserved: 0
.... 0... = Reserved: 0
....1 .... = Privacy: Data confidentiality required
....0. .... = Short Preamble: Not Allowed
.... .0.. .... = Critical Update Flag: False
.... 0... .... = Nontransmitted BSSIDs Critical Update Flag: False
....0 .... = Spectrum Management: Not Implemented
.... ..0. .... = QoS: Not Implemented
.... 0... .... = Automatic Power Save Delivery: Not Implemented
...0 .... = Radio Measurement: Not Implemented
..0. .... = EPD: Not Implemented
.0.. .... = Reserved: 0
0... .... = Reserved: 0
Tagged parameters (275 bytes)
Tag: SSID parameter set: "KMS-wpa2"
Tag: Supported Rates 6(B), 9, 12(B), 18, 24(B), 36, 48, 54, [Mbit/sec]
Tag: DS Parameter set: Current Channel: 165
Tag: Traffic Indication Map (TIM): DTIM 0 of 1 bitmap
Tag: RSN Information
Tag: Mobility Domain
Tag: HT Capabilities (802.11n D1.10)
Tag: HT Information (802.11n D1.10)
Tag: Extended Capabilities (10 octets)
Tag: VHT Capabilities
Tag: VHT Operation
Ext Tag: HE Capabilities
Ext Tag: HE Operation
Ext Tag: MU EDCA Parameter Set
Tag: Vendor Specific: Microsoft Corp.: WMM/WME: Parameter Element
Tag Number: Vendor Specific (221)
Tag length: 24
OUI: 00:50:f2 (Microsoft Corp.)
Vendor Specific OUI Type: 2
Type: WMM/WME (0x02)
WME Subtype: Parameter Element (1)
WME Version: 1
WME QoS Info: 0x88
1... .... = U-APSD: Enabled
.... 1000 = Parameter Set Count: 0x8
.000 .... = Reserved: 0x0
Reserved: 00
Ac Parameters ACI 0 (Best Effort), ACM no, AIFSN 3, ECWmin/max 4/10 (CWmin/max 15/1023), TXOP 0
Ac Parameters ACI 1 (Background), ACM no, AIFSN 7, ECWmin/max 4/10 (CWmin/max 15/1023), TXOP 0
Ac Parameters ACI 2 (Video), ACM no, AIFSN 2, ECWmin/max 3/4 (CWmin/max 7/15), TXOP 94
Ac Parameters ACI 3 (Voice), ACM no, AIFSN 2, ECWmin/max 2/3 (CWmin/max 3/7), TXOP 47
Tag: Vendor Specific: Qualcomm Inc.
Tag: Vendor Specific: Qualcomm Inc.
Tag: Vendor Specific: Aruba, a Hewlett Packard Enterprise Company: Unknown (Data: 0809)

Association Request
Client

```
> Frame 9736: 116 bytes on wire (928 bits), 116 bytes captured (928 bits)
> Radiotap Header v0, Length 36
> 802.11 radio information
v IEEE 802.11 Association Request, Flags: ........C
    Type/Subtype: Association Request (0x0000)
  > Frame Control Field: 0x0000
    .000 0000 0010 1100 = Duration: 44 microseconds
    Receiver address: ArubaHewlett_8b:1f:60 (94:64:24:8b:1f:60)
    Destination address: ArubaHewlett_8b:1f:60 (94:64:24:8b:1f:60)
    Transmitter address: Cisco_41:9c:37 (00:23:33:41:9c:37)
    Source address: Cisco_41:9c:37 (00:23:33:41:9c:37)
    BSS Id: ArubaHewlett_8b:1f:60 (94:64:24:8b:1f:60)
    .... .... .... 0000 = Fragment number: 0
    1100 0001 0001 .... = Sequence number: 3089
    Frame check sequence: 0xc05337b9 [unverified]
    [FCS Status: Unverified]
    [WLAN Flags: ........C]
v IEEE 802.11 Wireless Management
  > Fixed parameters (4 bytes)
  v Tagged parameters (48 bytes)
    > Tag: SSID parameter set:
    > Tag: Supported Rates 6(B), 9, 12(B), 18, 24(B), 36, 48, 54, [Mbit/sec]
    > Tag: Power Capability Min: 55, Max: -86
    > Tag: QoS Capability
    > Tag: Vendor Specific: Cisco Systems, Inc: Aironet Unknown (1) (1)
    v Tag: Vendor Specific: Microsoft Corp.: WMM/WME: Information Element
        Tag Number: Vendor Specific (221)
        Tag length: 7
        OUI: 00:50:f2 (Microsoft Corp.)
        Vendor Specific OUI Type: 2
        Type: WMM/WME (0x02)
        WME Subtype: Information Element (0)
        WME Version: 1
      v WME QoS Info: 0x0f
          .00. .... = Max SP Length: WMM AP may deliver all buffered frames (MSDUs and MMPDUs) (0x0)
          .... 1... = AC_BE: WMM delivery and trigger enabled
          .... .1.. = AC_BK: WMM delivery and trigger enabled
          .... ..1. = AC_VI: WMM delivery and trigger enabled
          .... ...1 = AC_VO: WMM delivery and trigger enabled
          0..0 .... = Reserved: 0x0
```

Cisco IP Phone 8821

All AC's enabled and triggered

```
> Frame 1090: 216 bytes on wire (1728 bits), 216 bytes captured (1728 bits)
> 802.11 radio information
v IEEE 802.11 Association Request, Flags: ........C
    Type/Subtype: Association Request (0x0000)
  > Frame Control Field: 0x0000
    .000 0000 0011 1100 = Duration: 60 microseconds
    Receiver address: ArubaHewlett_f8:27:30 (34:8a:12:f8:27:30)
    Destination address: ArubaHewlett_f8:27:30 (34:8a:12:f8:27:30)
    Transmitter address: Intel_f1:49:51 (00:91:9e:f1:49:51)
    Source address: Intel_f1:49:51 (00:91:9e:f1:49:51)
    BSS Id: ArubaHewlett_f8:27:30 (34:8a:12:f8:27:30)
    .... .... .... 0000 = Fragment number: 0
    0000 0000 0001 .... = Sequence number: 1
    Frame check sequence: 0xa2ec02de [unverified]
    [FCS Status: Unverified]
    [WLAN Flags: ........C]
EE 802.11 Wireless Management
  Fixed parameters (4 bytes)
  Tagged parameters (184 bytes)
  > Tag: SSID parameter set: "KMS-wpa2"
  > Tag: Supported Rates 6, 9, 12, 18, 24, 36, 48, 54, [Mbit/sec]
  > Tag: Power Capability Min: 0, Max: 15
  > Tag: HT Capabilities (802.11n D1.10)
  > Tag: RSN Information
  > Tag: Mobility Domain
  > Tag: Supported Operating Classes
  > Tag: RM Enabled Capabilities (5 octets)
  > Tag: Extended Capabilities (14 octets)
  > Tag: VHT Capabilities
  v Tag: Vendor Specific: Microsoft Corp.: WMM/WME: Information Element
      Tag Number: Vendor Specific (221)
      Tag length: 7
      OUI: 00:50:f2 (Microsoft Corp.)
      Vendor Specific OUI Type: 2
      Type: WMM/WME (0x02)
      WME Subtype: Information Element (0)
      WME Version: 1
    v WME QoS Info: 0x0f
        .00. .... = Max SP Length: WMM AP may deliver all buffered frames (MSDUs and MMPDUs) (0x0)
        .... 1... = AC_BE: WMM delivery and trigger enabled
        .... .1.. = AC_BK: WMM delivery and trigger enabled
        .... ..1. = AC_VI: WMM delivery and trigger enabled
        .... ...1 = AC_VO: WMM delivery and trigger enabled
        0..0 .... = Reserved: 0x0
  > Tag: Vendor Specific: Intel Wireless Network Group
  > Ext Tag: HE Capabilities
```

Windows Client
Intel AX210 chipset

Verify information on AP

```
AP655-Multiclient# sh ap association
Association Table
-----------------
Name               bssid             mac               auth  assoc  aid  l-int  essid     vlan-id  phy_cap              phy             assoc. time  num assoc  Flags
----               -----             ---               ----  -----  ---  -----  -----     -------  -------              ---             -----------  ---------  -----
AP655-Multiclient  34:8a:12:f8:27:30  00:91:9e:ef:92:3c  y     y      2    250    KMS-wpa2  1        5GHz-HE-160-2ss-RKVM 5GHz-HE-20-2ss  36s          1          WVRMUT
```

```
AP655-Multiclient# sh ap debug client-table
Client Table
------------
MAC                ESSID     BSSID             Assoc_State  HT_State  AID  PS_State    UAPSD            TWT    Tx_Pkts  Rx_Pkts  PS_Qlen  Tx_Retries  Tx_Rate  Rx_Rate  Last_ACK_SNR
Last_Rx_SNR  TX_Chains  Tx_Timestamp            Rx_Timestamp             MFP Status  (C,R)  Idle time  Client health (C/R)  Tx_Bytes  Rx_Bytes
---                ------    -----             -----------  --------  ---  --------    -----            ---    -------  -------  -------  ----------  -------  -------  ------------
-----------  ---------  ------------            ------------             ----------  ------  ---------  -------------------  --------  --------
00:91:9e:ef:92:3c  KMS-wpa2  34:8a:12:f8:27:30  Associated   AvsEeBbM  0x2  Awake       (1,1,1,1,all,0)  (0,0)  699      1346     0        59          143      243      31           48
      2[0x3]     Fri Aug  4 23:43:45 2023  Fri Aug  4 23:43:45 2023  (0,0)                15021120   100/87                515445    89012

Num of associated clients: 2
UAPSD:(VO,VI,BK,BE,Max SP,0 Len)
```

Maximum Service Period Length (MAX SP Length)
Client

```
> Frame 9736: 116 bytes on wire (928 bits), 116 bytes captured (928 bits)
> Radiotap Header v0, Length 36
> 802.11 radio information
> IEEE 802.11 Association Reque
v IEEE 802.11 Wireless Managemer
  > Fixed parameters (4 bytes)
  v Tagged parameters (48 bytes
    > Tag: SSID parameter set:
    > Tag: Supported Rates 6(B
    > Tag: Power Capability Mi
    > Tag: QoS Capability
    > Tag: Vendor Specific: Cisco Systems, Inc: Aironet Unknown (1) (1)
    v Tag: Vendor Specific: Microsoft Corp.: WMM/WME: Information Element
        Tag Number: Vendor Specific (221)
        Tag length: 7
        OUI: 00:50:f2 (Microsoft Corp.)
        Vendor Specific OUI Type: 2
        Type: WMM/WME (0x02)
        WME Subtype: Information Element (0)
        WME Version: 1
      v WME QoS Info: 0x0f
          .00. .... = Max SP Length: WMM AP may deliver all buffered frames (MSDUs and MMPDUs) (0x0)
          .... 1... = AC_BE: WMM delivery and trigger enabled
          .... .1.. = AC_BK: WMM delivery and trigger enabled
          .... ..1. = AC_VI: WMM delivery and trigger enabled
          .... ...1 = AC_VO: WMM delivery and trigger enabled
          0..0 .... = Reserved: 0x0
```

MAX SP LENGTH

Bit 5	Bit 6	Description
0	0	AP may deliver all buffered MSDUs, A-MSDUs, and MMPDUs
1	0	AP may deliver a max of 2 MSDUs, A-MSDUs, and MMPDUs per SP
0	1	AP may deliver a max of 4 MSDUs, A-MSDUs, and MMPDUs per SP
1	1	AP may deliver a max of 6 MSDUs, A-MSDUs, and MMPDUs per SP

Let's have a closer look..

REF	Cisco_41:9c:37	ArubaHewlett_8b:1f:60
0.000004		Cisco_41:9c:37 (00:23:33:41
0.000008	15.111.200.64	10.33.67.203
0.000012		ArubaHewlett_8b:1f:60 (94:6
0.015018	10.33.67.203	15.111.200.64
0.015031		Cisco_41:9c:37 (00:23:33:41
0.081512	Cisco_41:9c:37	ArubaHewlett_8b:1f:60

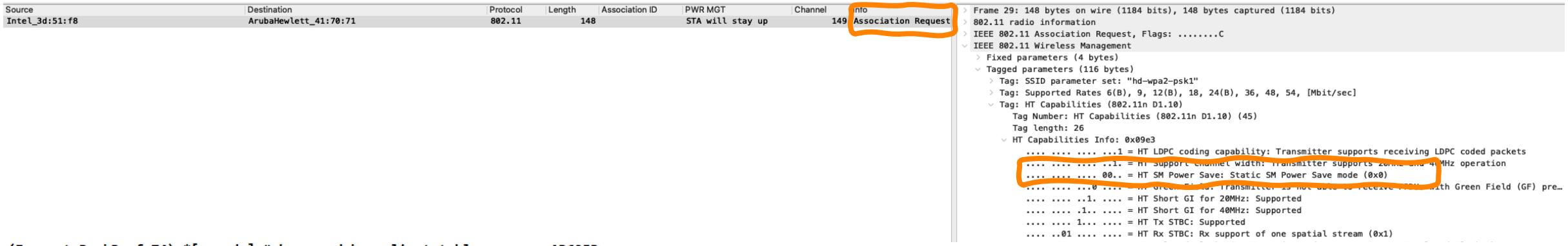
```
> Frame 36173: 156 bytes on wire (1248 bits), 156 bytes captured (1248 bits)
> Radiotap Header v0, Length 58
> 802.11 radio information
v IEEE 802.11 QoS Data, Flags: ...P...TC
    Type/Subtype: QoS Data (0x0028)
  v Frame Control Field: 0x8811
      .... ..00 = Version: 0
      .... 10.. = Type: Data frame (2)
      1000 .... = Subtype: 8
    v 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... .... = +HTC/Order flag: Not strictly ordered
    .000 0000 0010 1100 = Duration: 44 microseconds
    Receiver address: ArubaHewlett_8b:1f:60 (94:64:24:8b:1f:60)
    Transmitter address: Cisco_41:9c:37 (00:23:33:41:9c:37)
    Destination address: ArubaHewlett_c8:d3:40 (64:e8:81:c8:d3:40)
    Source address: Cisco_41:9c:37 (00:23:33:41:9c:37)
    BSS Id: ArubaHewlett_8b:1f:60 (94:64:24:8b:1f:60)
    STA address: Cisco_41:9c:37 (00:23:33:41:9c:37)
    .... .... .... 0000 = Fragment number: 0
    0100 0000 1101 .... = Sequence number: 1037
    Frame check sequence: 0x3c5236a7 [unverified]
    [FCS Status: Unverified]
    [WLAN Flags: ...P...TC]
  v Qos Control: 0x0000
      .... .... .... 0000 = TID: 0
      [.... .... .... .000 = Priority: Best Effort (Best Effort) (0)]
      .... .... ...0 .... = QoS bit 4: Bits 8-15 of QoS Control field are TXOP Duration Requested
      .... .... .00. .... = Ack Policy: Normal Ack (0x0)
      .... .... 0... .... = Payload Type: MSDU
      0000 0000 .... .... = TXOP Duration Requested: 0 (no TXOP requested)
> Logical-Link Control
> Internet Protocol Version 4, Src: 10.33.67.203, Dst: 15.111.200.64
> Internet Control Message Protocol
```

Ping reply and sleep again

MIMO power save mode
Spatial Multiplexing Power Save (SMPS)

- Used on almost every Windows device running Intel WiFi chipset
  - Default setting is auto
  - Older Intels uses S-SMPS
  - Most of them D-SMPS (*since 802.11n day*)
- SM power save allows MIMO (802.11n or later) capable devices to power down all but one of RF chain
  - In this case a 4x4 MIMO device can power down three of the four RF chains to save power
- SM power save provides two methods:
  - Static
    - Client enables only one Rx chain and the AP transmits frames to the client at one spatial stream data rates
  - Dynamic
    - Client listens on 1 Rx Chain, but toggles to all chains upon Rx a frame destined to the client
    - Client goes back to 1 Rx Chain mode if there are no more frames destined for the client.
    - AP can use RTS-CTS exchange or send any frame at the single spatial stream rate to make the client enable all chains

Static Mode



Source	Destination	Protocol	Length	Association ID	PWR MGT	Channel	Info
Intel_3d:51:f8	ArubaHewlett_41:70:71	802.11	148		STA will stay up	149	Association Request

```
Frame 29: 148 bytes on wire (1184 bits), 148 bytes captured (1184 bits)
802.11 radio information
IEEE 802.11 Association Request, Flags: ........C
IEEE 802.11 Wireless Management
  Fixed parameters (4 bytes)
  Tagged parameters (116 bytes)
    Tag: SSID parameter set: "hd-wpa2-psk1"
    Tag: Supported Rates 6(B), 9, 12(B), 18, 24(B), 36, 48, 54, [Mbit/sec]
    Tag: HT Capabilities (802.11n D1.10)
      Tag Number: HT Capabilities (802.11n D1.10) (45)
      Tag length: 26
      HT Capabilities Info: 0x09e3
        .... .... .... ...1 = HT LDPC coding capability: Transmitter supports receiving LDPC coded packets
        .... .... .... ..1. = HT Support channel width: Transmitter supports 20MHz and 40MHz operation
        .... .... .... 00.. = HT SM Power Save: Static SM Power Save mode (0x0)
        .... .... ...0 .... = HT Green Field: Transmitter is not able to receive PPDUs with Green Field (GF) pre…
        .... .... ..1. .... = HT Short GI for 20MHz: Supported
        .... .... .1.. .... = HT Short GI for 40MHz: Supported
        .... .... 1... .... = HT Tx STBC: Supported
        .... ..01 .... .... = HT Rx STBC: Rx support of one spatial stream (0x1)
```

```
(Fremont-PeakPerf-74) *[mynode] #show ap debug client-table ap-name AP635P

Client Table
------------
MAC                ESSID         BSSID              Assoc_State  HT_State     AID  PS_State    UAPSD           TWT    Tx_Pkts  Rx_Pkts  PS_Qlen  Tx_Retries  Tx_Rate  Rx_Rate  Last_ACK_SNR
Last_Rx_SNR  TX_Chains  Tx_Timestamp              Rx_Timestamp              MFP Status (C,R)  Idle time  Client health (C/R)
---                ------        -----              -----------  --------     ---  --------    -----           ---    -------  -------  -------  ----------  -------  -------  ------------
-----------  ---------  ------------              ------------              ----------------  ---------  ------------------
34:02:86:3d:51:f8  hd-wpa2-psk1  cc:88:c7:41:70:71  Associated   AWvSsEeBbQM  0x1  Power-save  (0,0,0,0,N/A,0)  (0,0)  126      212      0        7           135      300      44
46           2[0x3]     Thu Mar 14 11:39:02 2024  Thu Mar 14 11:39:12 2024  (0,0)             11         30/30


Num of associated clients: 1
UAPSD:(VO,VI,BK,BE,Max SP,Q Len)
TWT:(iTWT sessions num, bTWT groups num)
HT  Flags: A - LDPC Coding; B - TX STBC; D - Delayed BA; G - Greenfield
           I - HT40 Intolerant; M - Max A-MSDU; N - A-MPDU disabled
           Q - Static SM PS; R - Dynamic SM PS; S - Short GI 40; W - 40 MHz
           b - RX STBC; s - Short GI 20; t - turbo-rates (256-QAM)
VHT Flags: C - 160MHz/80+80MHz; E - Beamformee;  V - Short GI 160
           c - 80MHz; e - Beamformer; v - Short GI 80
HT_State shows client's original capabilities (not operational capabilities)
MFP Status: C - 1 if the station is MFP capable; R - 1 if the station has negotiated MFP
(Fremont-PeakPerf-74) *[mynode] #
```

Dynamic mode

Source	Destination	Protocol	Length	Association ID	PWR MGT	Channel	Info
Intel_3d:51:f8	ArubaHewlett_41:70:71	802.11	148		STA will stay up	149	Association Request

```
Frame 74: 148 bytes on wire (1184 bits), 148 bytes captured (1184 bits)
802.11 radio information
IEEE 802.11 Association Request, Flags: ........C
IEEE 802.11 Wireless Management
  Fixed parameters (4 bytes)
  Tagged parameters (116 bytes)
    Tag: SSID parameter set: "hd-wpa2-psk1"
    Tag: Supported Rates 6(B), 9, 12(B), 18, 24(B), 36, 48, 54, [Mbit/sec]
    Tag: HT Capabilities (802.11n D1.10)
      Tag Number: HT Capabilities (802.11n D1.10) (45)
      Tag length: 26
      HT Capabilities Info: 0x09e7
        .... .... .... ...1 = HT LDPC coding capability: Transmitter supports receiving LDPC coded packets
        .... .... .... ..1. = HT Support channel width: Transmitter supports 20MHz and 40MHz operation
        .... .... .... 01.. = HT SM Power Save: Dynamic SM Power Save mode (0x1)
        .... .... ...0 .... = HT Greenfield: Transmitter is not capable of transmitting PPDUs with Green Field (GF)
        .... .... ..1. .... = HT Short GI for 20MHz: Supported
        .... .... .1.. .... = HT Short GI for 40MHz: Supported
        .... .... 1... .... = HT Tx STBC: Supported
        .... ..01 .... .... = HT Rx STBC: Rx support of one spatial stream (0x1)
        .... .0.. .... .... = HT Delayed Block ACK: Transmitter does not support HT-Delayed BlockAck
        .... 1... .... .... = HT Max A-MSDU length: 7935 bytes
        ...0 .... .... .... = HT DSSS/CCK mode in 40MHz: Won't/Can't use of DSSS/CCK in 40 MHz
        ..0. .... .... .... = HT PSMP Support: Won't/Can't support PSMP operation
        .0.. .... .... .... = HT Forty MHz Intolerant: Use of 40 MHz transmissions unrestricted/allowed
        0... .... .... .... = HT L-SIG TXOP Protection support: Not supported
```

```
(Fremont-PeakPerf-74) *[mynode] #show ap debug client-table ap-name AP635P

Client Table
------------
MAC               ESSID         BSSID              Assoc_State  HT_State     AID  PS_State    UAPSD           TWT    Tx_Pkts  Rx_Pkts  PS_Qlen  Tx_Retries  Tx_Rate  Rx_Rate  Last_ACK_SNR
Last_Rx_SNR  TX_Chains  Tx_Timestamp              Rx_Timestamp             MFP Status (C,R)  Idle time  Client health (C/R)
---               -----         -----              -----------  --------     ---  --------    -----           ---    -------  -------  -------  ----------  -------  -------  ------------
-----------  ---------  ------------              ------------             ----------------  ---------  ------------------
34:02:86:3d:51:f8  hd-wpa2-psk1  cc:88:c7:41:70:71  Associated   AWvSsEeBbRM  0x1  Power-save  (0,0,0,0,N/A,0)  (0,0)  233      754      0        20          243      240      36
40           2[0x3]     Wed Mar 13 15:27:09 2024  Wed Mar 13 15:27:40 2024  (0,0)            15         50/59


Num of associated clients: 2
UAPSD:(VO,VI,BK,BE,Max SP,Q Len)
TWT:(iTWT sessions num, bTWT groups num)
HT  Flags: A - LDPC Coding; B - TX STBC; D - Delayed BA; G - Greenfield
           I - HT40 Intolerant; M - Max A-MSDU; N - A-MPDU disabled
           Q - Static SM PS; R - Dynamic SM PS  S - Short GI 40; W - 40 MHz
           b - RX STBC; s - Short GI 20; t - turbo-rates (256-QAM)
VHT Flags: C - 160MHz/80+80MHz; E - Beamformee;  V - Short GI 160
           c - 80MHz; e - Beamformer; v - Short GI 80
HT_State shows client's original capabilities (not operational capabilities)
MFP Status: C - 1 if the station is MFP capable; R - 1 if the station has negotiated MFP
(Fremont-PeakPerf-74) *[mynode] #
```

Dynamic mode

Packet	Source	Destination	Absolute Time	BSSID	Delta Time	Size	Protocol	Spatial Streams	Summary
1969	Intel:3D:51:F8	CC:88:C7:41:70:71	15:17:23.582899	CC:88:C7:41:70:71	0.100088	30	802.11 QoS Null ...	1	FC=T...P...,SN= 0,FN= 0
1970	CC:88:C7:41:70:71	Intel:3D:51:F8	15:17:23.583899		0.001000	14	802.11 Ack	1	FC=.....
1971	Intel:3D:51:F8	CC:88:C7:41:70:71	15:17:28.600261	CC:88:C7:41:70:71	5.016362	30	802.11 QoS Null ...	1	FC=T.....,SN= 0,FN= 0
1972	CC:88:C7:41:70:71	Intel:3D:51:F8	15:17:28.600261		0.000000	14	802.11 Ack	1	FC=.....
1973	CC:88:C7:41:70:71	Intel:3D:51:F8	15:17:28.602263		0.002002	20	802.11 RTS	1	FC=.....
1974	Intel:3D:51:F8	CC:88:C7:41:70:71	15:17:28.602263		0.000000	14	802.11 CTS	1	FC=.....
1975	ArubaaHewlettPa...	Intel:3D:51:F8	15:17:28.602263	CC:88:C7:41:70:71	0.000000	1082	802.11 Encrypted	2	FC=.F....W.,SN= 115,FN= 0
1976	Intel:3D:51:F8	CC:88:C7:41:70:71	15:17:28.602263		0.000000	32	802.11 BA	1	FC=.....
1977	Intel:3D:51:F8	ArubaaHewlettPa...	15:17:28.603263	CC:88:C7:41:70:71	0.001001	1082	802.11 Encrypted	2	FC=T.....W.,SN= 282,FN= 0
1978	CC:88:C7:41:70:71	Intel:3D:51:F8	15:17:28.603263		0.000000	14	802.11 Ack	1	FC=.....

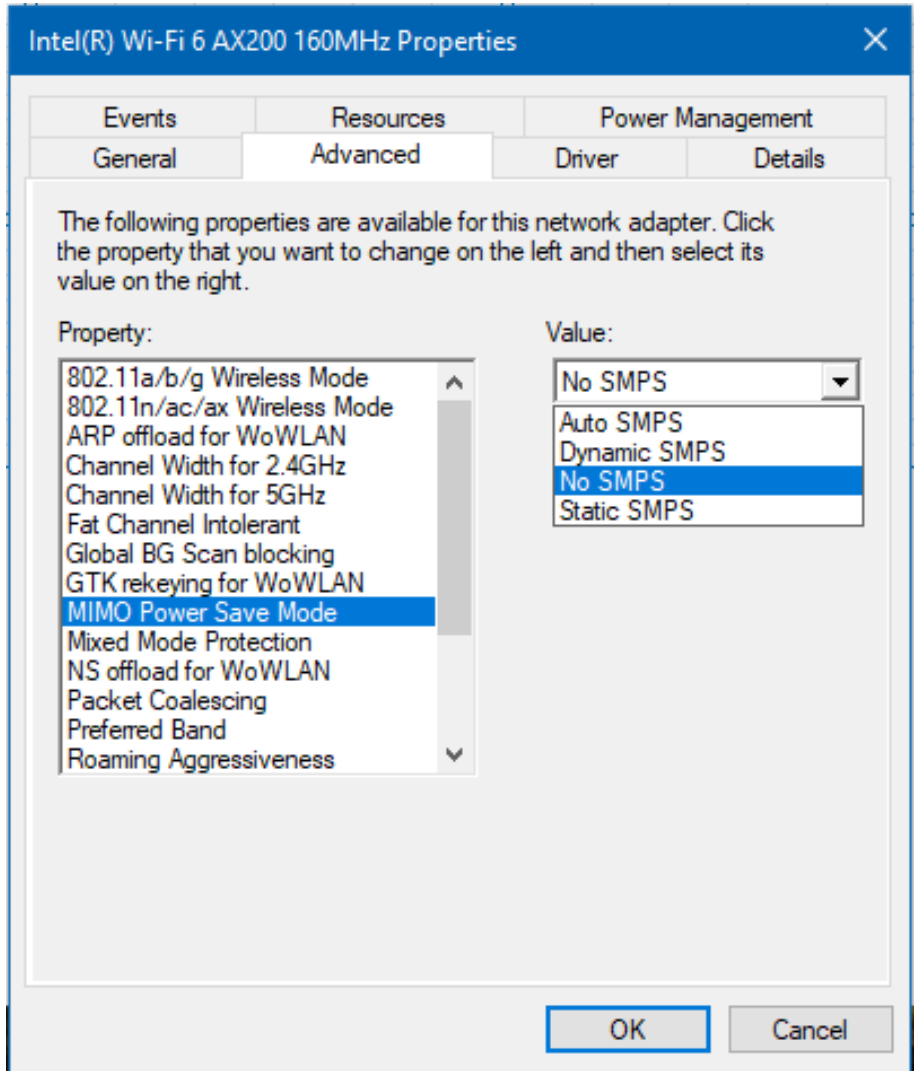
STA 5s before waking up in frame #1971

STA has to do successful RTS/CTS handshake to wake up all spatial streams on station

'From DS' TX is using 2ss to deliver echo request pkt

Above is instance of ping Echo request from wired side every 5s to Intel client

Intel Wireless Adapters



MIMO power save mode

MIMO power save mode, also known as spatial multiplexing power save (SMPS) mode, allows the client to save power by keeping one antenna in a receive idle state.

- **Auto SMPS** (default): The client decides automatically what SMPS mode to apply depends on different conditions.
- **Dynamic SMPS**: The client keeps only one antenna active. The access point (AP) must send request to send (RTS) packet to trigger the client to wake the sleeping radios/antenna before sending MIMO packets.
- **Static SMPS**: The client keeps only one antenna active and the AP cannot send MIMO packets to the client.
- **No SMPS**: The client always keeps all antennas active and the AP can send MIMO packets to the client.

Note	Some legacy APs may have compatibility issue with supporting the SMPS mode and may cause various link quality problems such as low throughput. Change this setting to **No SMPS** may help to work around the issue.

https://www.intel.com/content/www/us/en/support/articles/000005585/wireless/legacy-wireless-products.html

HOPE YOU'RE STILL AWAKE