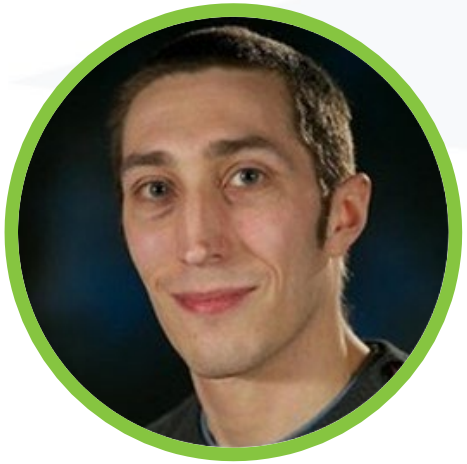
Analysing Roaming Protocols



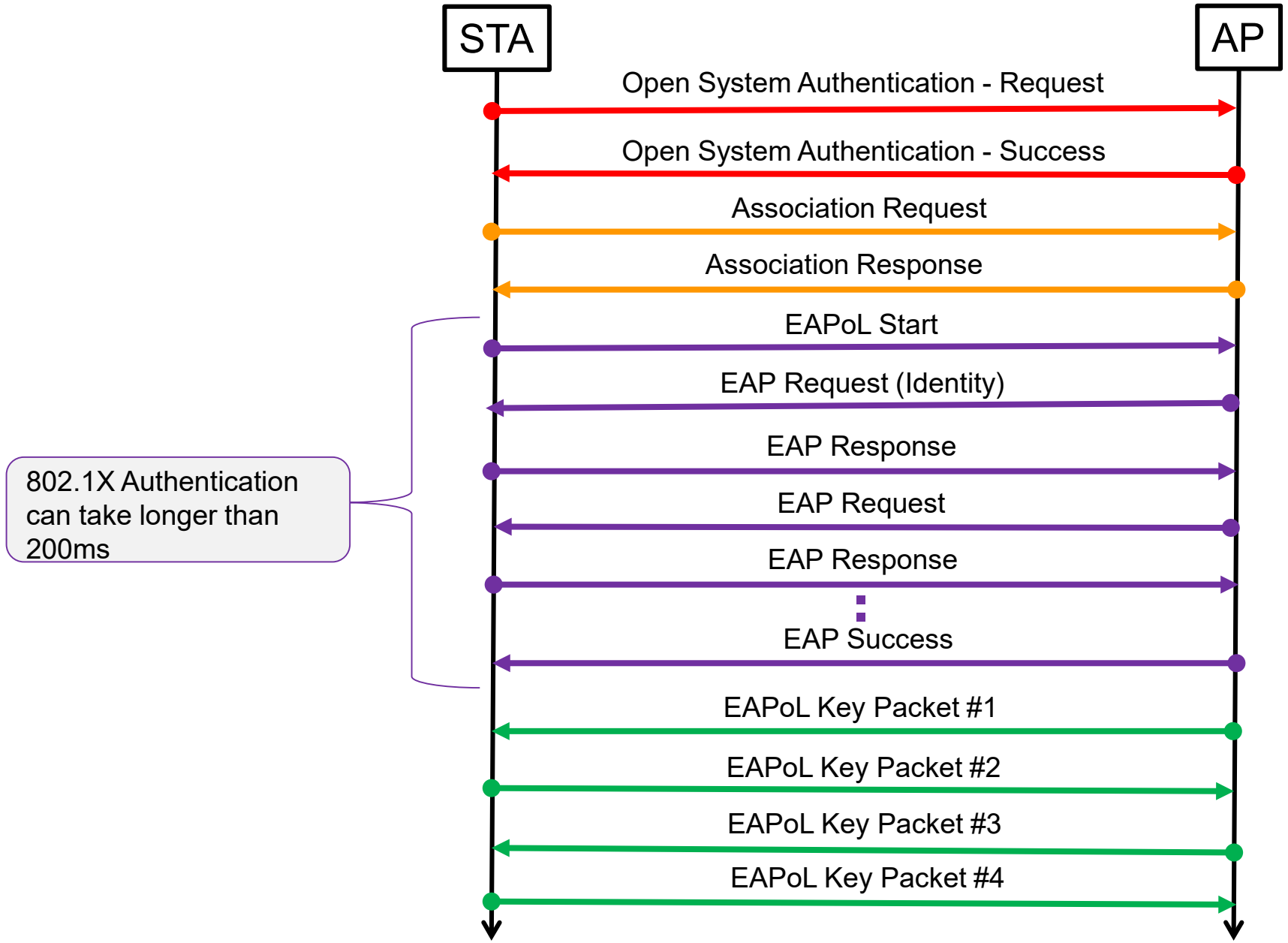
Head of Technical Operations | MarQuest

MackenzieWiFi

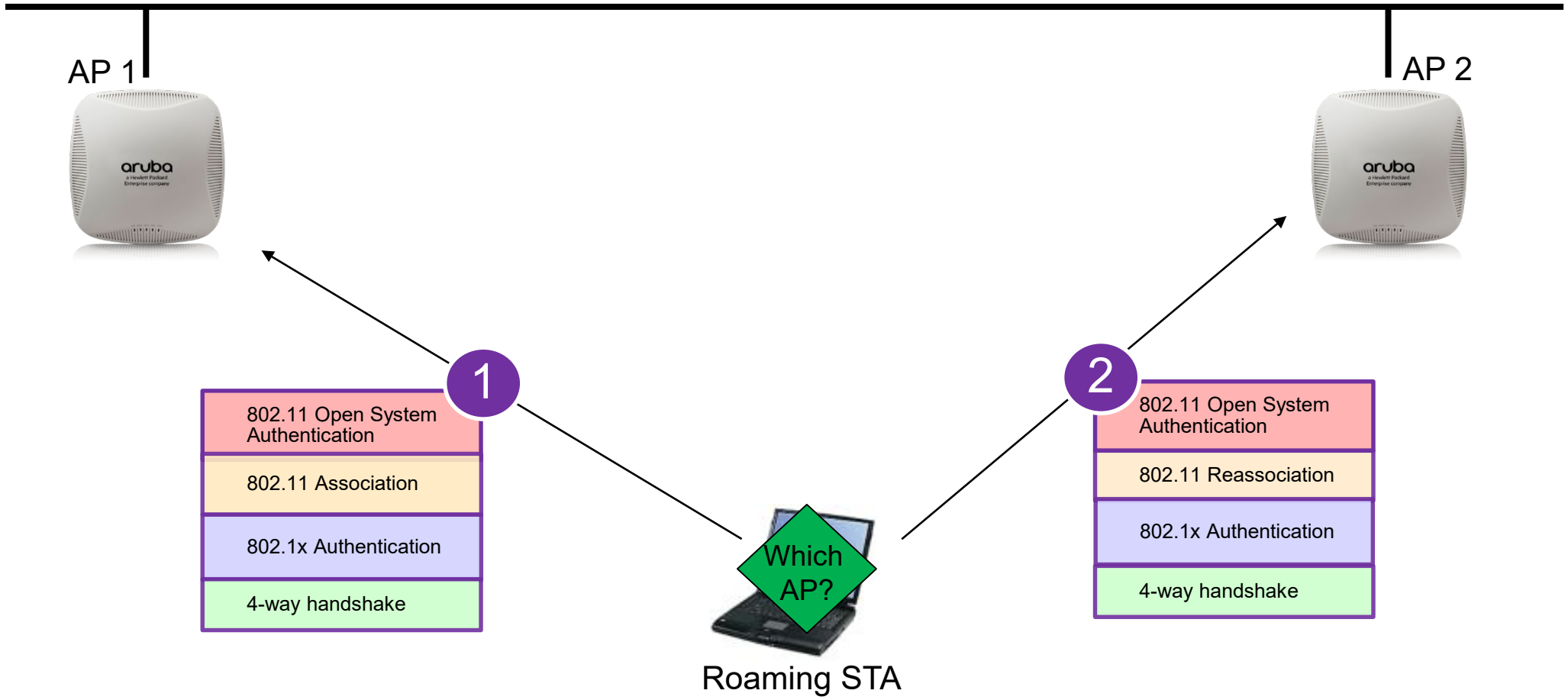
#WiFiDesignDay

by Ekahau and Open Reality

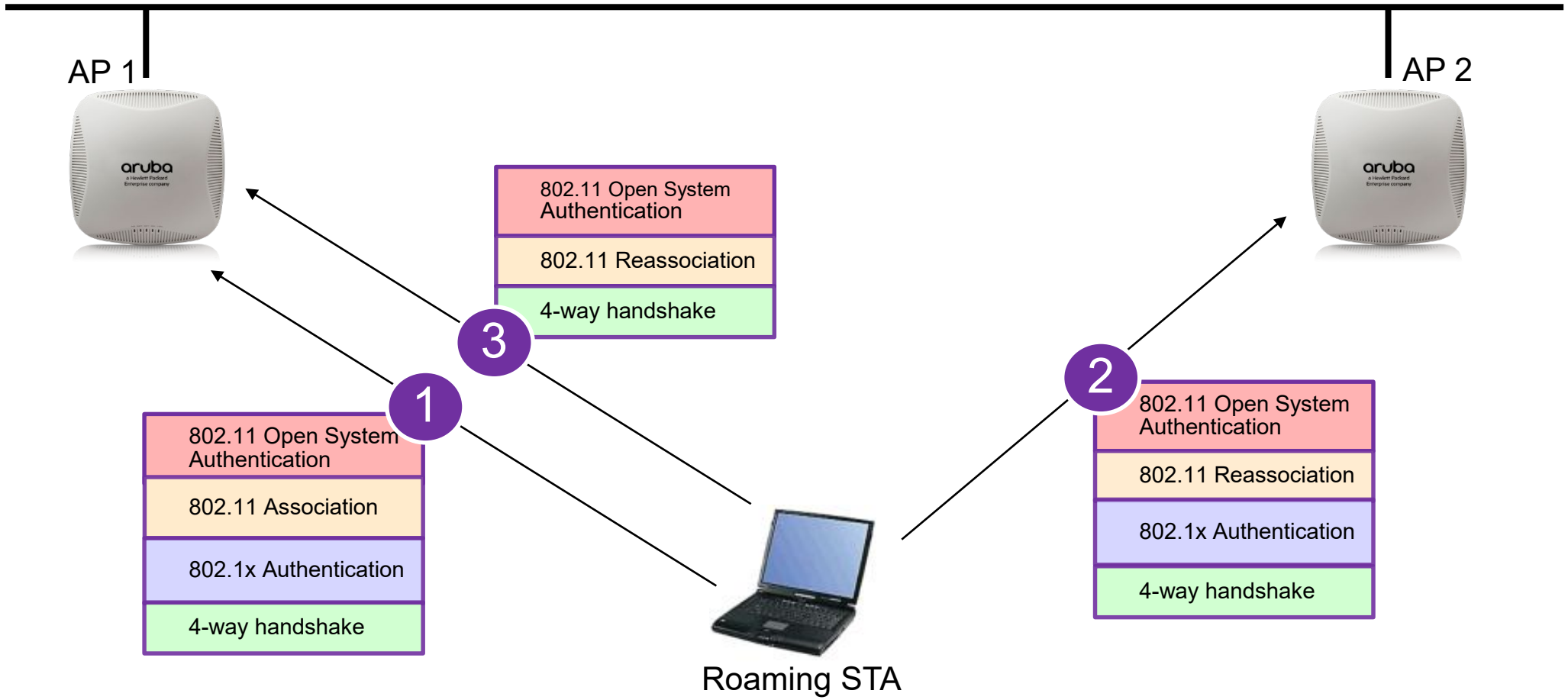
802.1X Association



Slow Roam



PMK Caching – “Fast-Roam-Back”



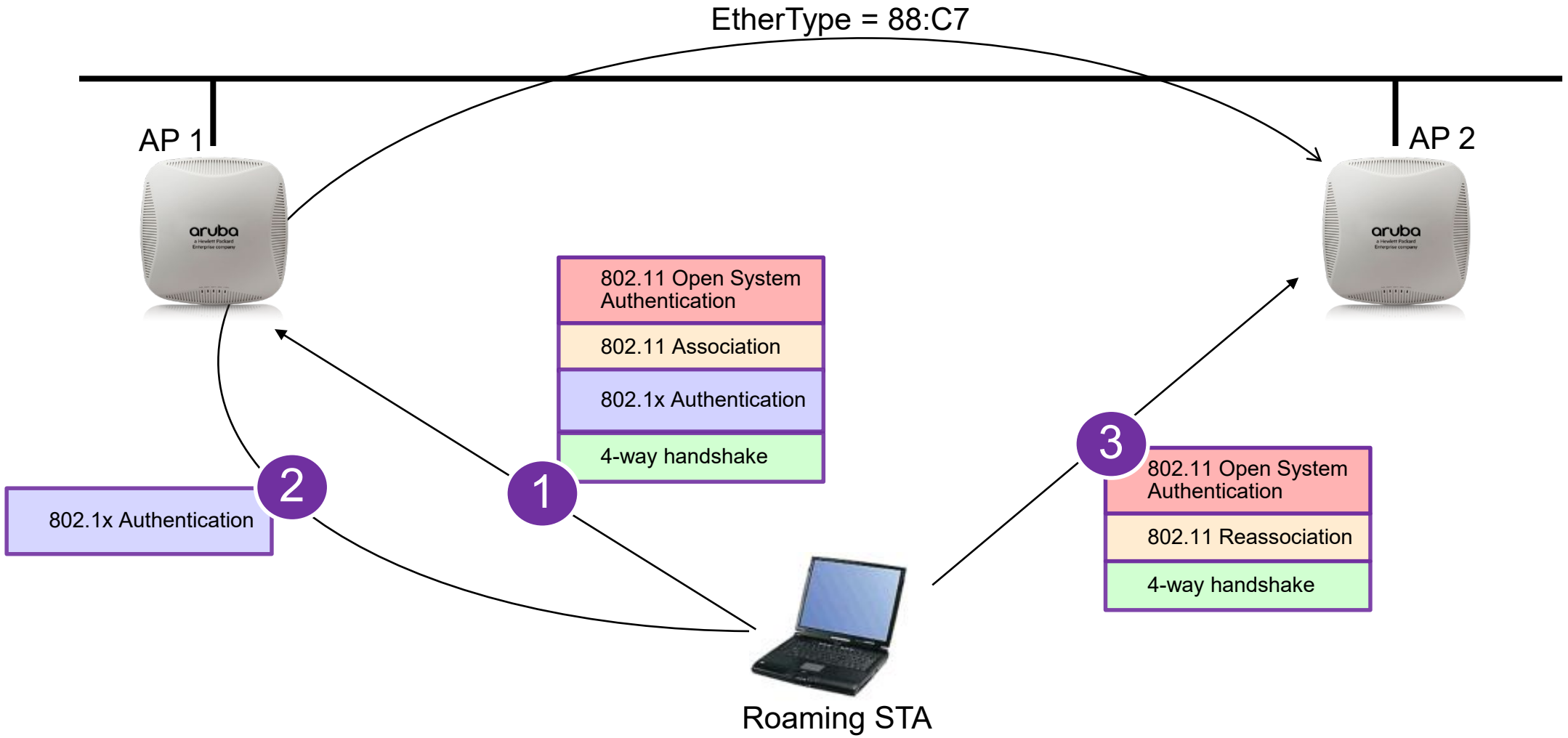
Reassociation RSN Element Decode

MarQuest Networking Support

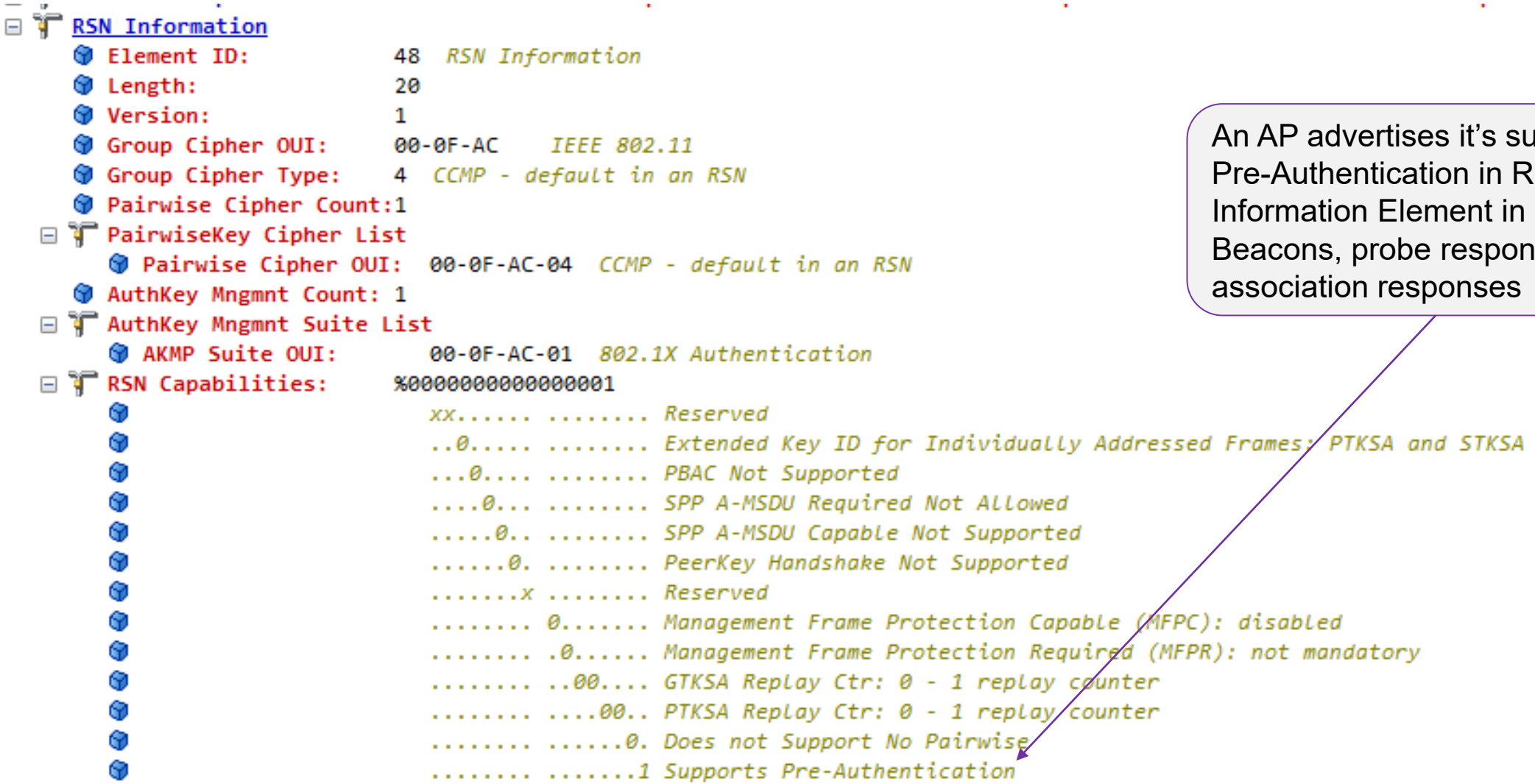
```
RSN Information
    Element ID:              48  RSN Information
    Length:                  38
    Version:                 1
    Group Cipher OUI:        00-0F-AC    IEEE 802.11
    Group Cipher Type:       4  CCMP - default in an RSN
    Pairwise Cipher Count:1
  PairwiseKey Cipher List
      Pairwise Cipher OUI:   00-0F-AC-04  CCMP - default in an RSN
    AuthKey Mngmnt Count: 1
  AuthKey Mngmnt Suite List
      AKMP Suite OUI:        00-0F-AC-01  802.1X Authentication
  RSN Capabilities:          %0000000000001100
                               xx..... ........ Reserved
                               ..0..... ........ Extended Key ID for Individually Addressed Frames: PTKSA and STKSA
                               ...0.... ........ PBAC Not Supported
                               ....0... ........ SPP A-MSDU Required Not Allowed
                               .....0.. ........ SPP A-MSDU Capable Not Supported
                               ......0. ........ PeerKey Handshake Not Supported
                               .......x ........ Reserved
                               ........ 0....... Management Frame Protection Capable (MFPC): disabled
                               ........ .0...... Management Frame Protection Required (MFPR): not mandatory
                               ........ ..00.... GTKSA Replay Ctr: 0 - 1 replay counter
                               ........ ....11.. PTKSA Replay Ctr: 3 - 16 replay counters
                               ........ ......0. Does not Support No Pairwise
                               ........ .......0 Does Not Support Pre-Authentication
    PMKID Count:             1
    PMKID:                   0x3195877E83278E25FA8C81A4400D617E
```

ID of Cached PMK

Pre-Authentication



Pre-Authentication Support



An AP advertises it's support for Pre-Authentication in RSN Information Element in Beacons, probe responses and association responses

Opportunistic Key Caching (OKC)

2

PMK

AP 1

AP 2

1

802.11 Open System Authentication

802.11 Association

802.1x Authentication

4-way handshake

Roaming STA

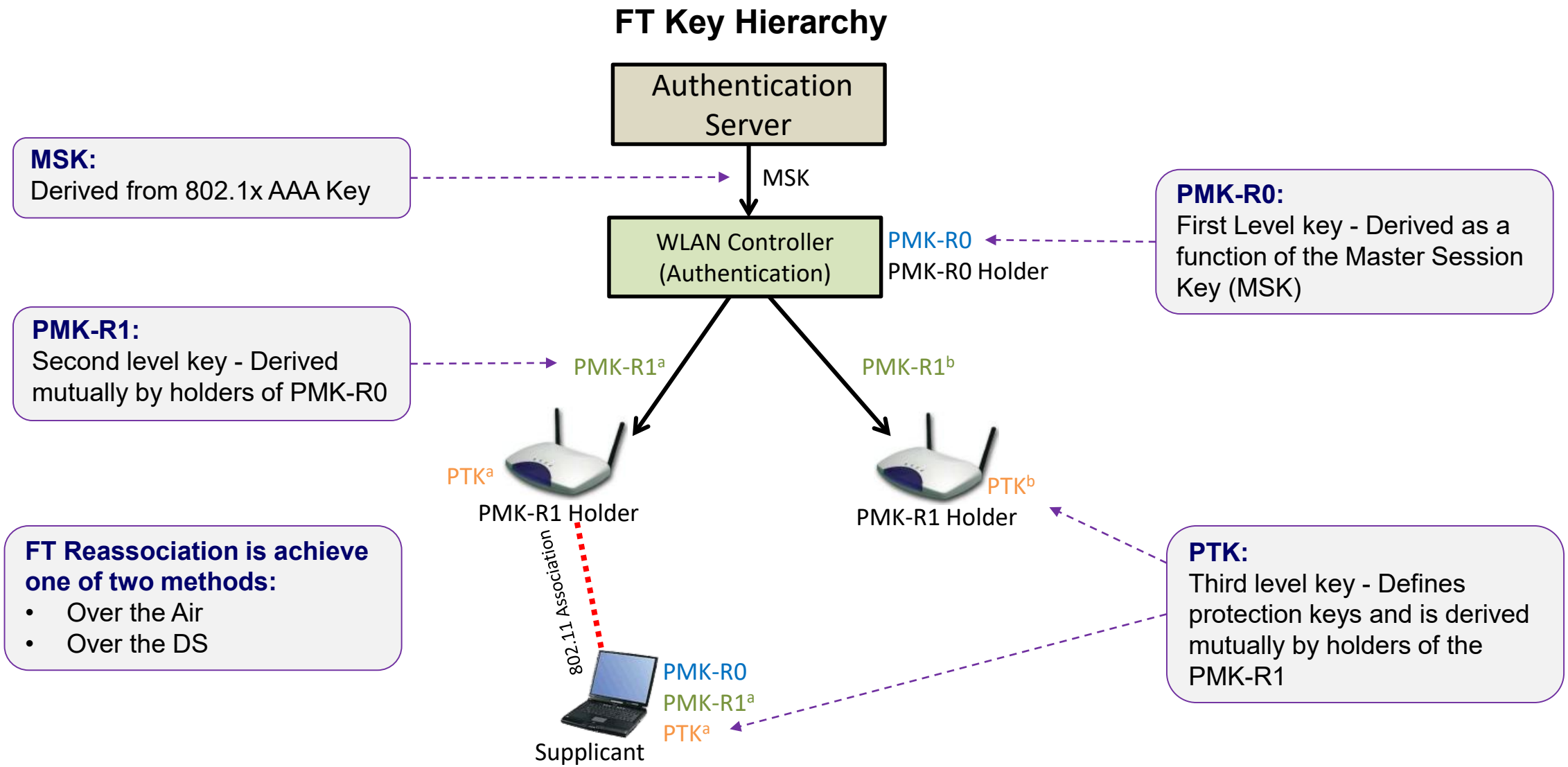
3

802.11 Open System Authentication

802.11 Reassociation

4-way handshake

Fast BSS Transition (FT) - 802.11r



MSK:
Derived from 802.1x AAA Key

PMK-R0:
First Level key - Derived as a function of the Master Session Key (MSK)

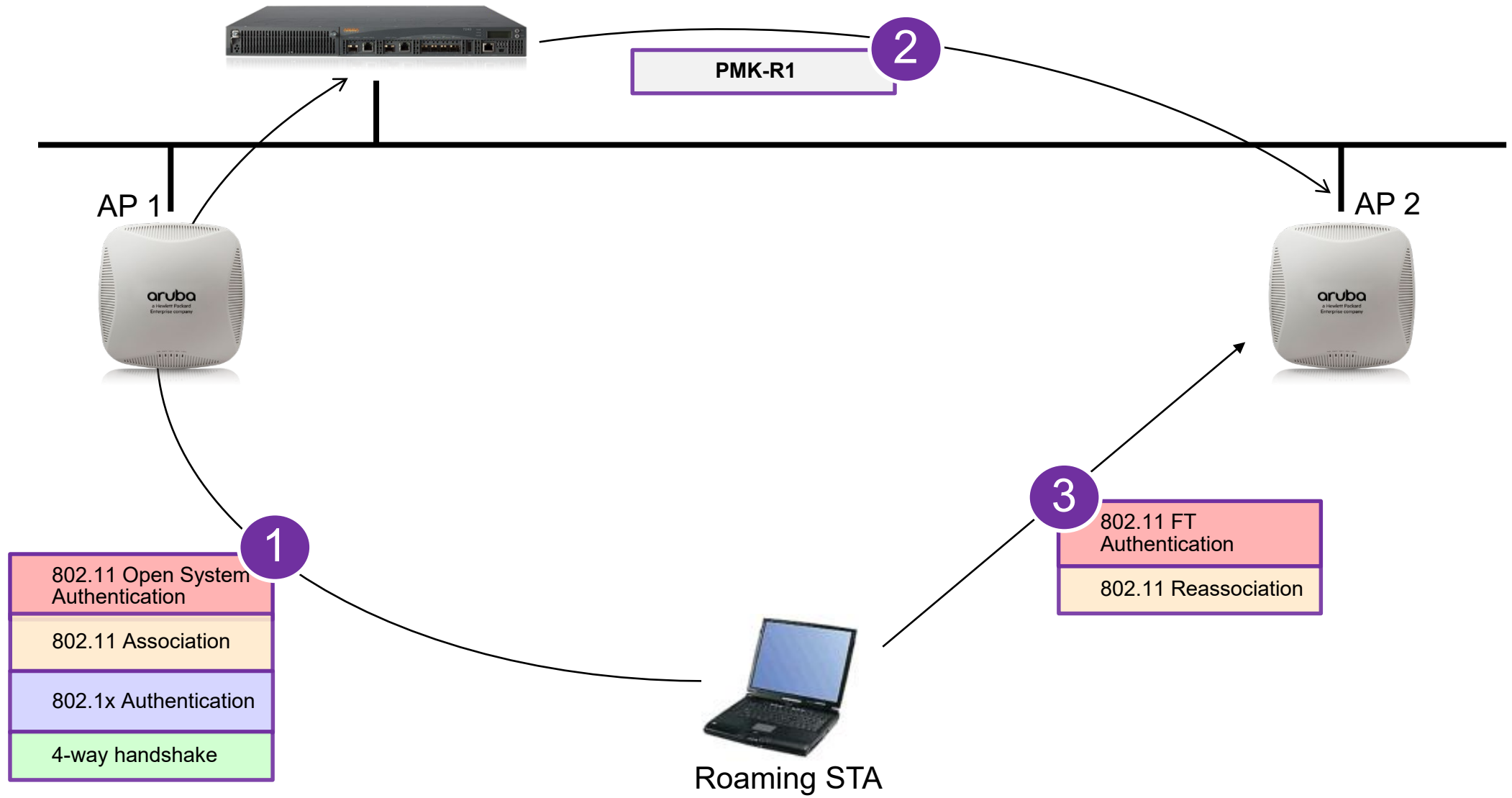
PMK-R1:
Second level key - Derived mutually by holders of PMK-R0

FT Reassociation is achieve one of two methods:

- Over the Air
- Over the DS

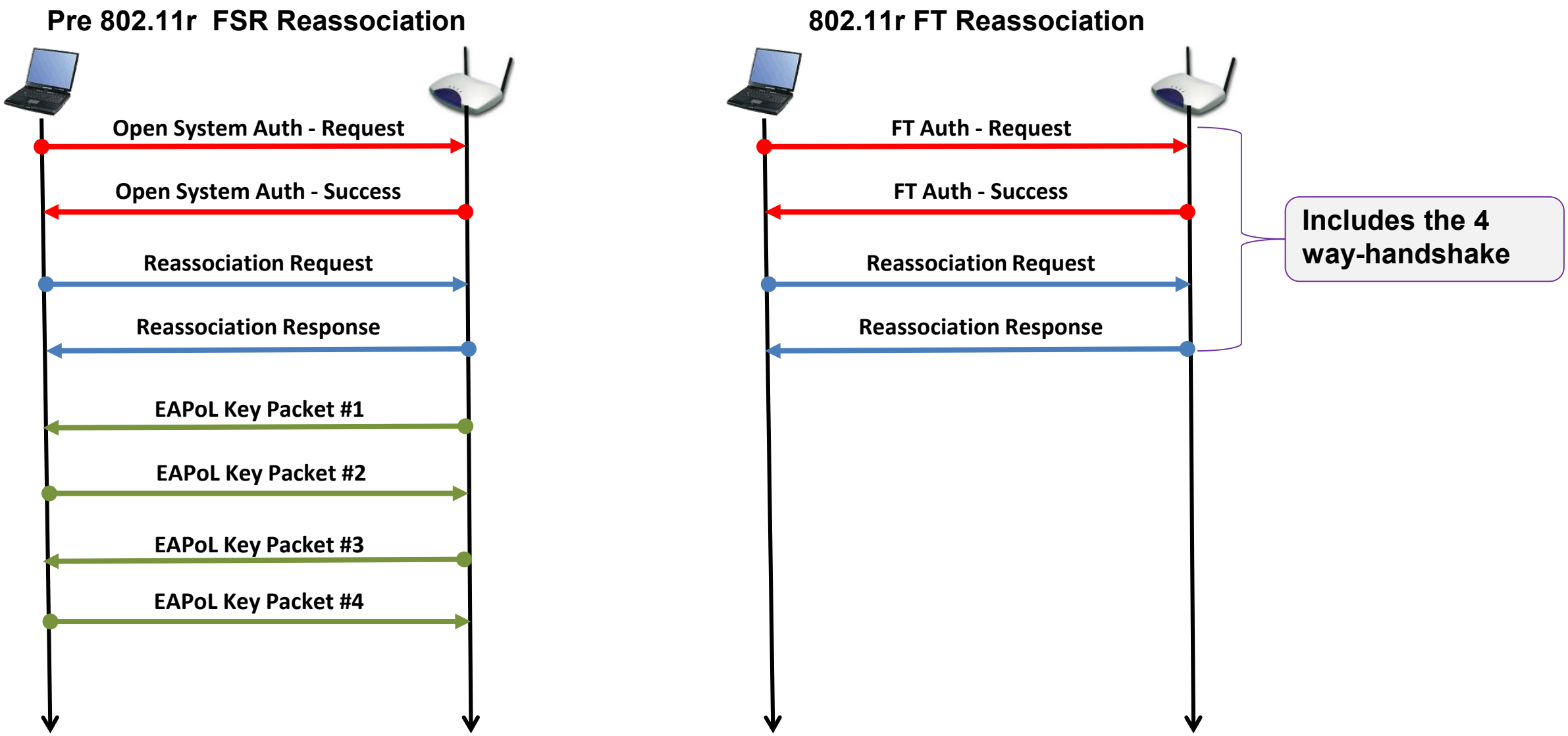
PTK:
Third level key - Defines protection keys and is derived mutually by holders of the PMK-R1

FT Over the Air

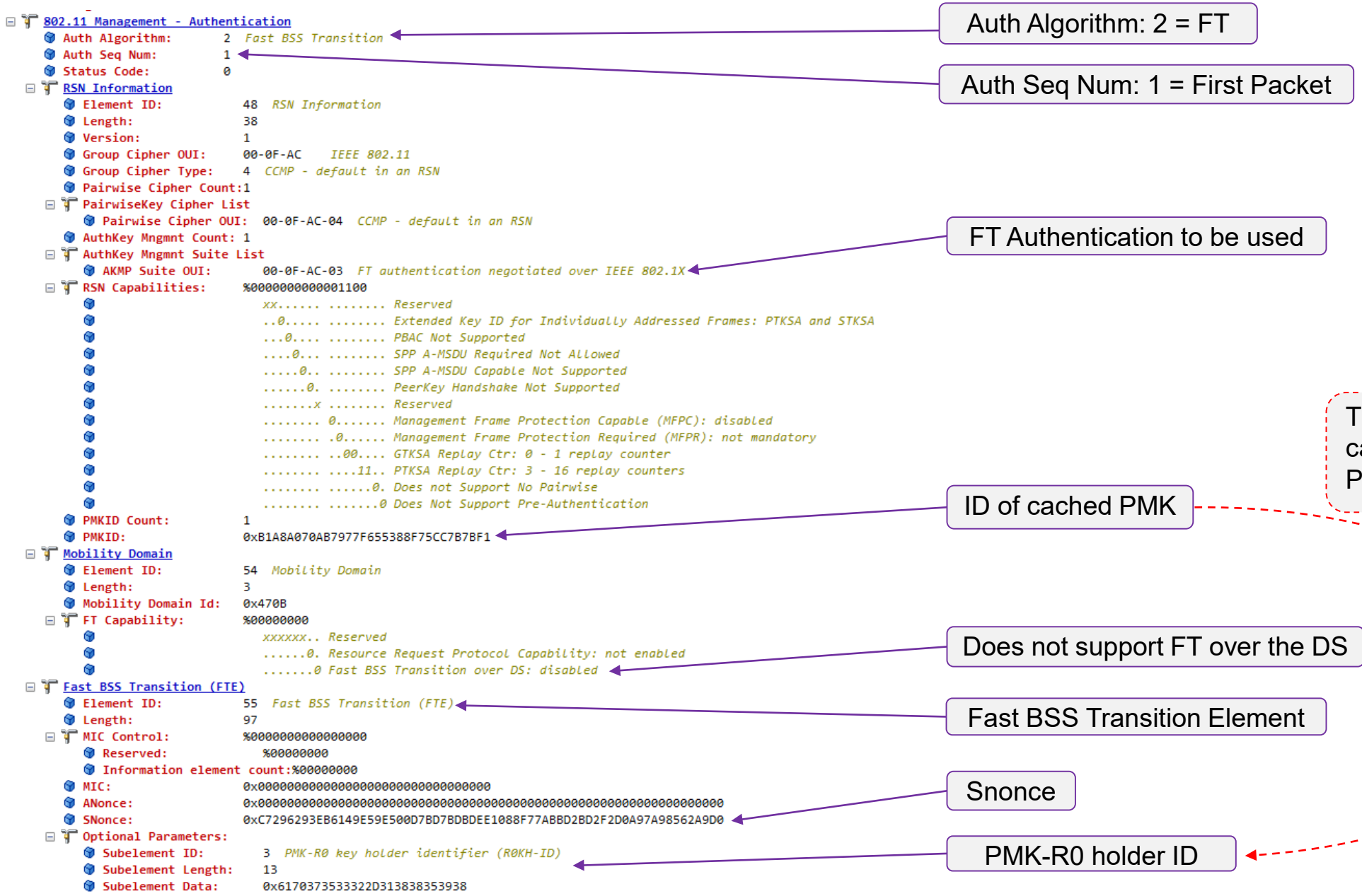


Pre 802.11r FSR vs FT Over the air

MarQuest Networking Support



FT Over the Air Packet #1



FT Over the Air Packet #2

```
802.11 Management - Authentication
    Auth Algorithm:        2  Fast BSS Transition
    Auth Seq Num:          2
    Status Code:           0
  Mobility Domain
      Element ID:          54  Mobility Domain
      Length:              3
      Mobility Domain Id:  0x470B
    FT Capability:         %00000000
                             xxxxxx.. Reserved
                             ......0. Resource Request Protocol Capability: not enabled
                             .......0 Fast BSS Transition over DS: disabled
  RSN Information
      Element ID:          48  RSN Information
      Length:              42
      Version:             1
      Group Cipher OUI:    00-0F-AC    IEEE 802.11
      Group Cipher Type:   4  CCMP - default in an RSN
      Pairwise Cipher Count:1
    PairwiseKey Cipher List
        Pairwise Cipher OUI:  00-0F-AC-04  CCMP - default in an RSN
      AuthKey Mngmnt Count: 2
    AuthKey Mngmnt Suite List
        AKMP Suite OUI:      00-0F-AC-01  802.1X Authentication
        AKMP Suite OUI:      00-0F-AC-03  FT authentication negotiated over IEEE 802.1X
    RSN Capabilities:      %0000000000000000
                             xx...... ........ Reserved
                             ..0..... ........ Extended Key ID for Individually Addressed Frames: PTKS
                             ...0.... ........ PBAC Not Supported
                             ....0... ........ SPP A-MSDU Required Not Allowed
                             .....0.. ........ SPP A-MSDU Capable Not Supported
                             ......0. ........ PeerKey Handshake Not Supported
                             .......x ........ Reserved
                             ........ 0....... Management Frame Protection Capable (MFPC): disabled
                             ........ .0...... Management Frame Protection Required (MFPR): not mandat
                             ........ ..00.... GTKSA Replay Ctr: 0 - 1 replay counter
                             ........ ....00.. PTKSA Replay Ctr: 0 - 1 replay counter
                             ........ ......0. Does not Support No Pairwise
                             ........ .......0 Does Not Support Pre-Authentication
      PMKID Count:         1
      PMKID:               0xB1A8A070AB7977F655388F75CC7B7BF1
  Fast BSS Transition (FTE)
      Element ID:          55  Fast BSS Transition (FTE)
      Length:              105
    MIC Control:           %0000000000000000
        Reserved:            %00000000
        Information element count:%00000000
      MIC:                 0x00000000000000000000000000000000
      ANonce:              0x144DE8F54AFE54D397B1ABBCE5558C39D91081D164280E05BB125D0CFE37B139
      SNonce:              0xC7296293EB6149E59E500D7BD7BDBDEE1088F77ABBD2BD2F2D0A97A98562A9D0
    Optional Parameters:
        Subelement ID:       1  PMK-R1 key holder identifier (R1KH-ID)
        Subelement Length:   6
        Subelement Data:     0x84248D2BEF40
        Subelement ID:       3  PMK-R0 key holder identifier (R0KH-ID)
        Subelement Length:   13
        Subelement Data:     0x6170373533322D313838353938
```

Auth Algorithm: 2 = FT

Auth Seq Num: 2 = Second Packet

The Authenticator has now derived the PNK-R1 Key and becomes a PMK-R1 Holder

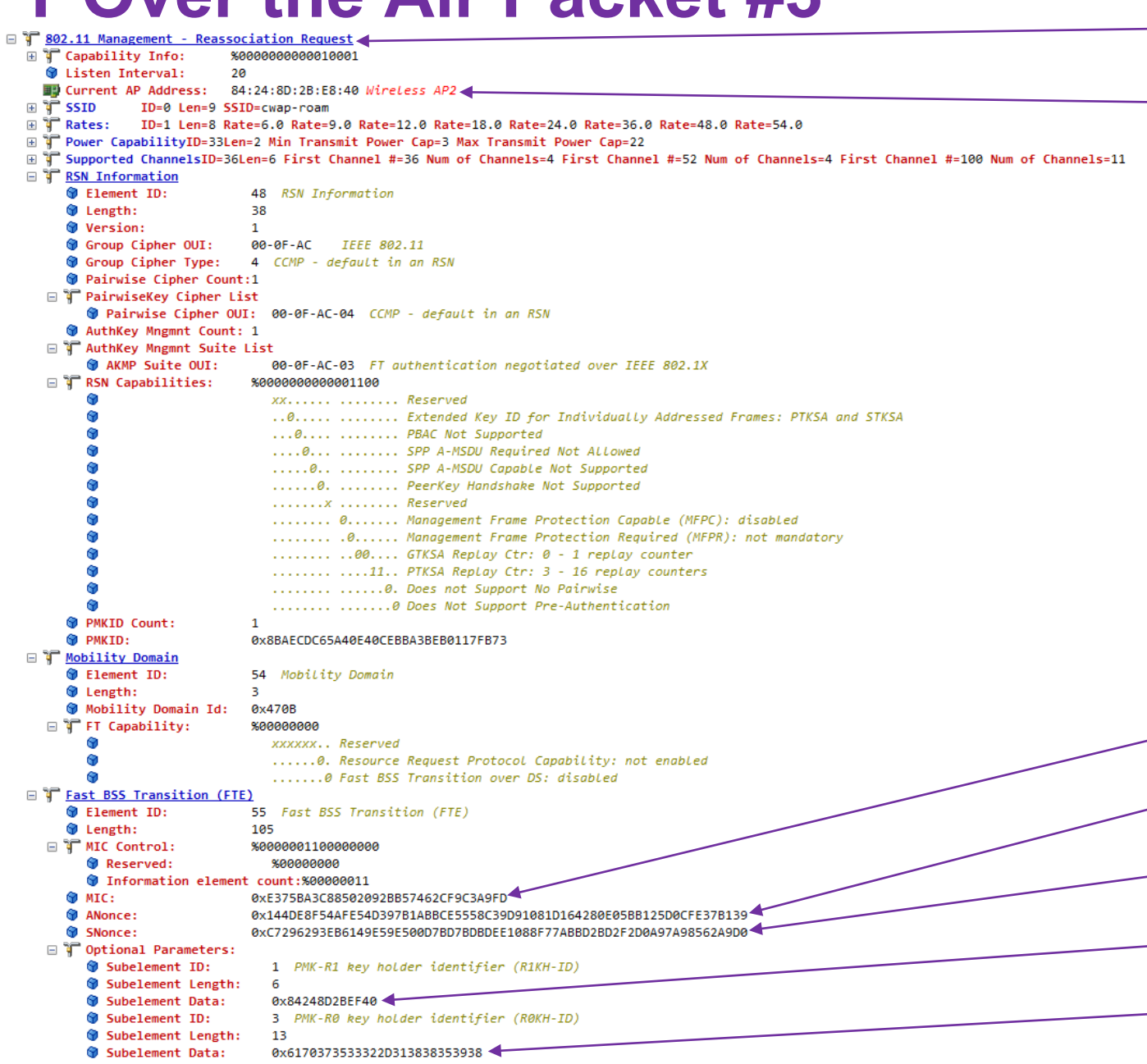
Anonce

Snonce

PMK-R1 holder ID

PMK-R0 holder ID

FT Over the Air Packet #3



Reassociation Request

Current AP BSSID

The Supplicant has now derived the PNK-R1 Key and becomes a PMK-R1 Holder.
The supplicant has also derived the PTK

MIC

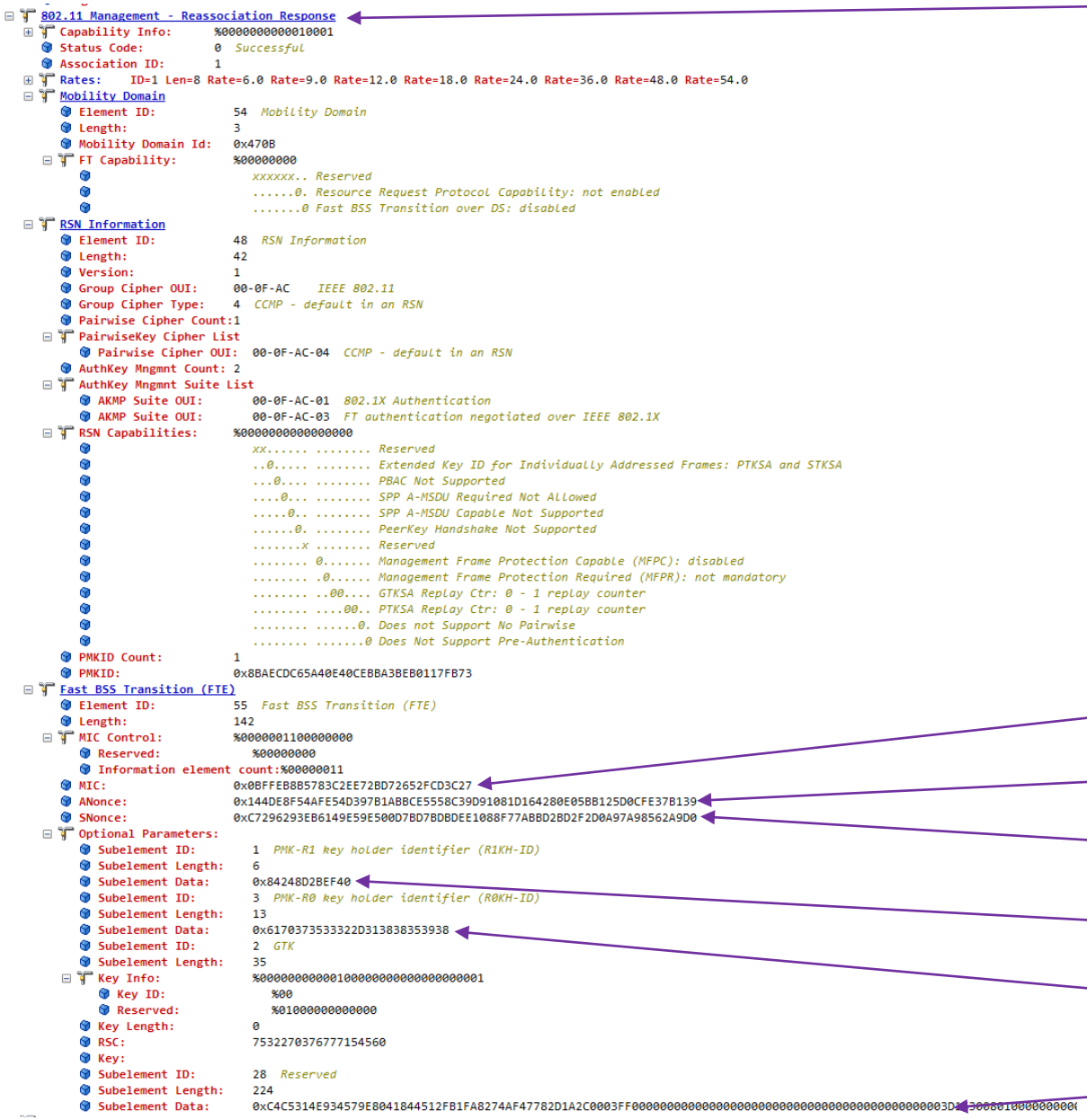
Anonce

Snonce

PMK-R1 holder ID

PMK-R0 holder ID

FT Over the Air Packet #4



Reassociation Response

The Supplicant has now derived the PMK-R1 Key and becomes a PMK-R1 Holder.
The supplicant has also derived the PTK

MIC

Anonce

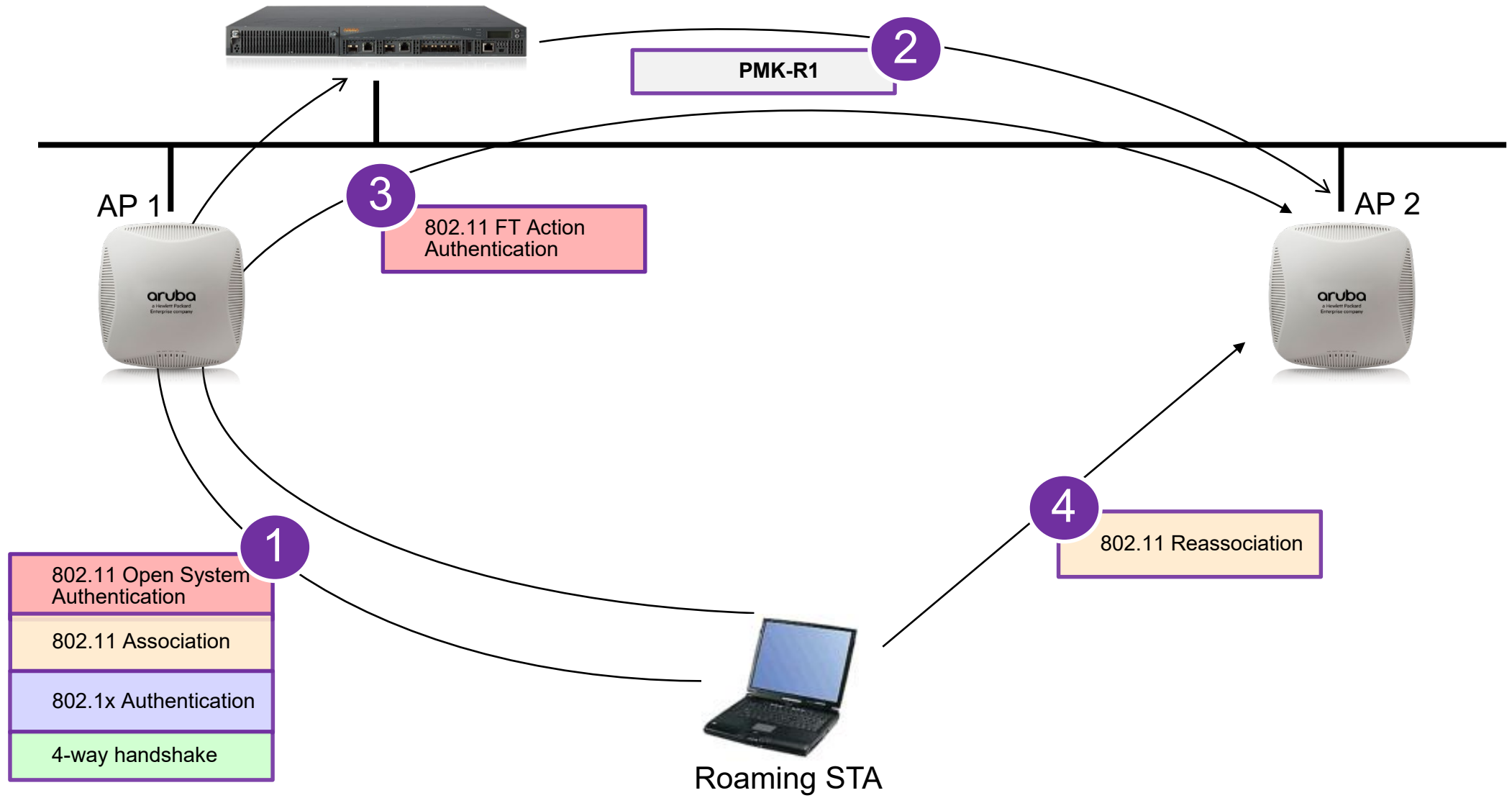
Snonce

PMK-R1 holder ID

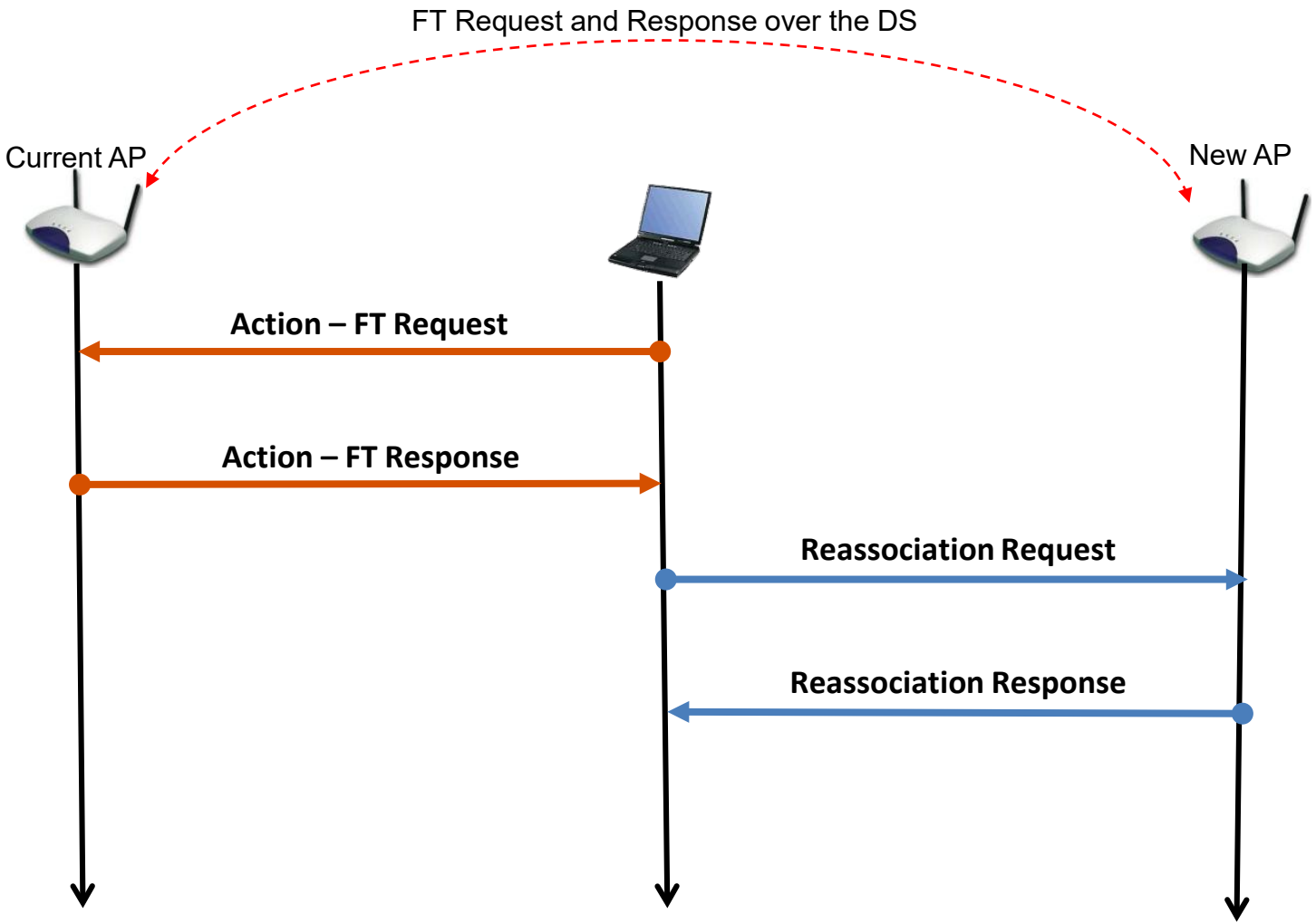
PMK-R0 holder ID

GTK encrypted in PTK

FT Over the DS



FT Over the DS Frame Exchange



802.11k – Radio Resource Measurement

802.11k and 802.11r work together to facilitate seamless roaming
Enables STAs to make informed roaming decisions

Capability Information Field

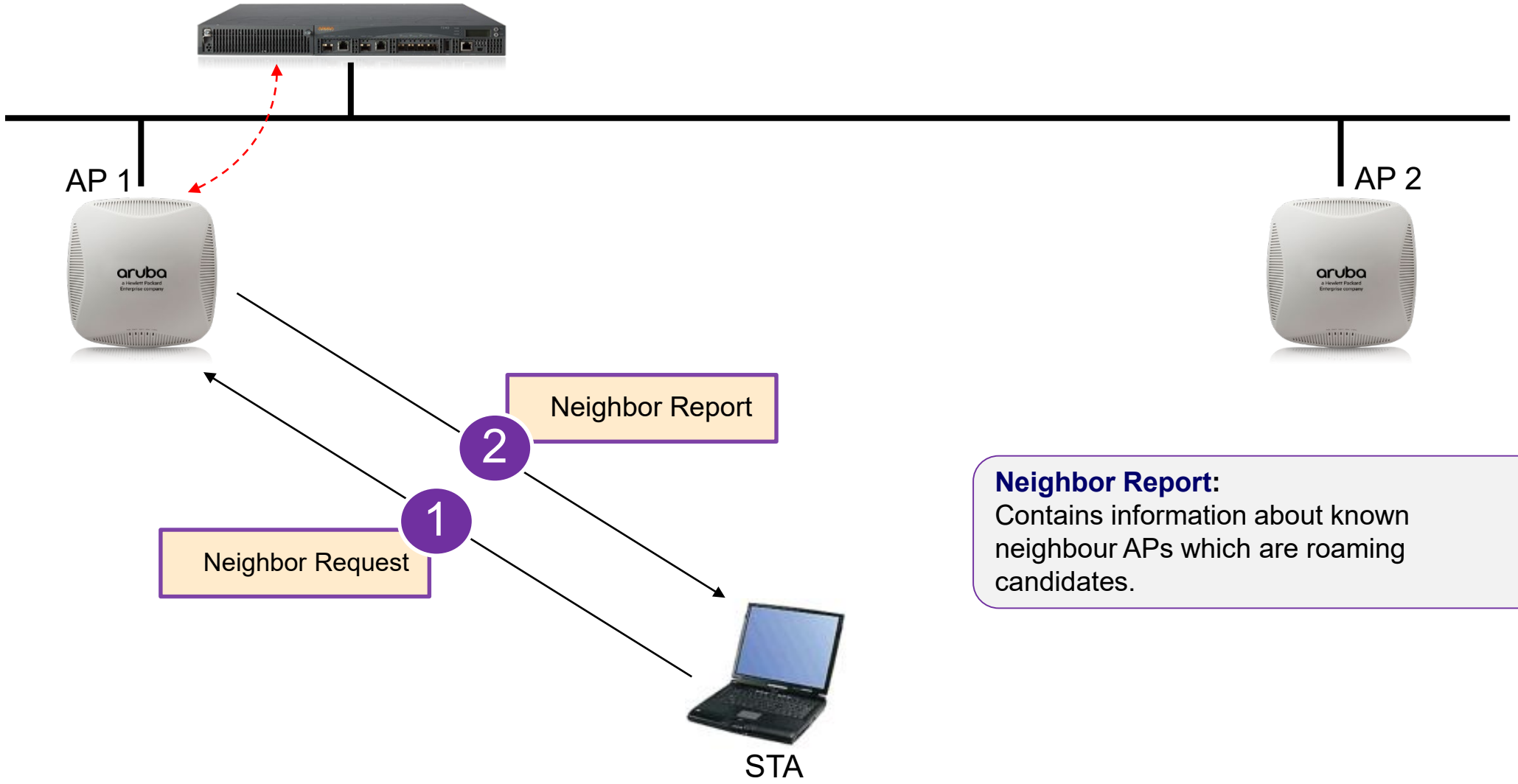
ESS	IBSS	CF Pollable	FC-Poll Request	Privacy	Short Preamble	Reserved	Reserved	Spectrum Management	QoS	Short Slot Time	APSD	Radio Measurement	Reserved	Delayed Block Ack	Immediate Block Ack
B0	B1	B2	B3	B4	B5	B6	B7	B8	B9	B10	B11	B12	B13	B14	B15

RRM Enabled Capabilities Element

Element ID = 70	Length = 5	RRM Enabled Capabilities
1	1	5

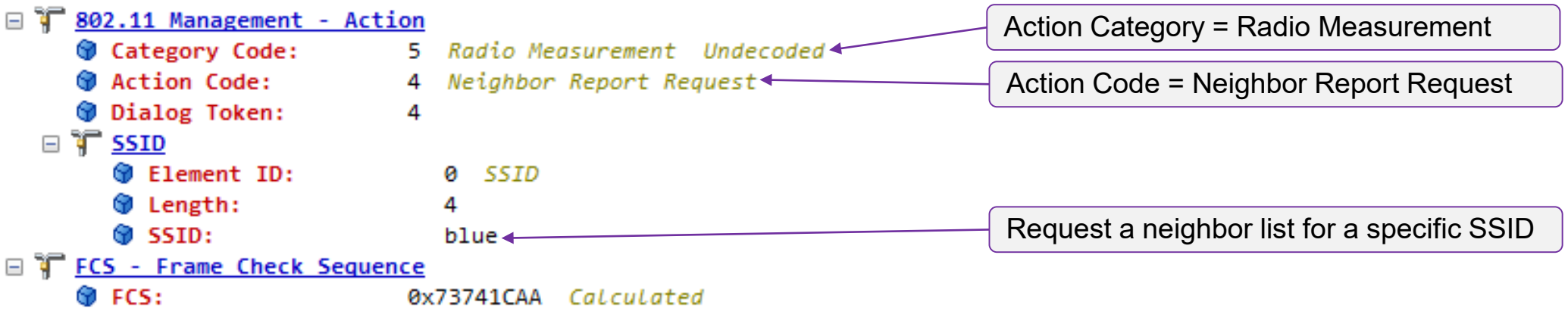
The Radio Measurement bit set to 1 in the Capability Information Field indicates general support for Radio Resource Measurement. Support for individual capabilities are indicated by a set of flag in the RRM Enabled Capabilities Element

Neighbor Report

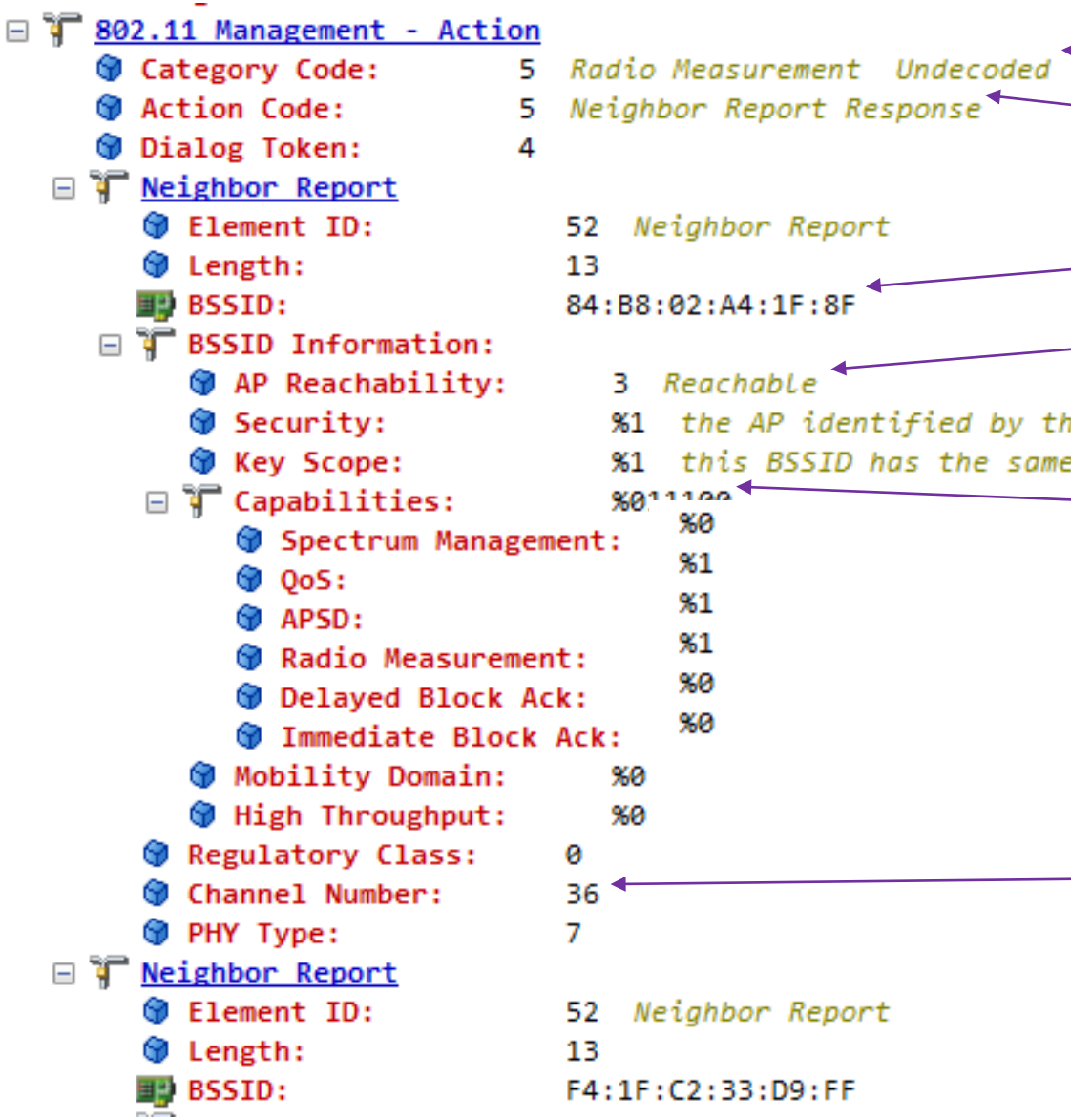


Neighbor Report:
Contains information about known neighbour APs which are roaming candidates.

Neighbour Request Decode



Neighbour Report Decode



Action Category = Radio Measurement

Action Code = Neighbor Report Response

Neighbor's BSSID

AP is reachable for preauthentication

Selected subset of the AP's Capability Information Field

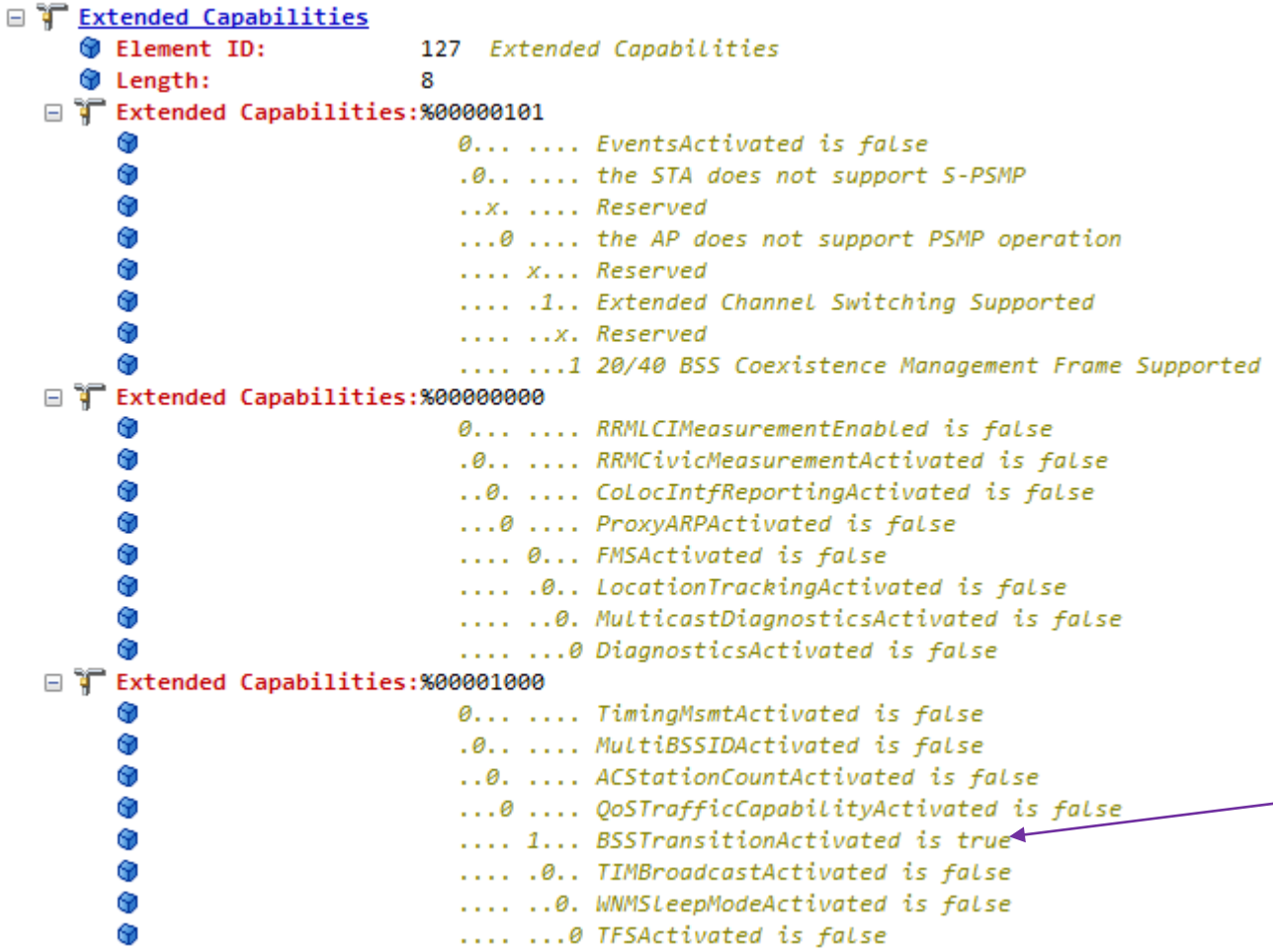
Channel number of new AP

By concentrating on just the APs in the Neighbor list, clients reduce their scanning activity (active probing or passively listening to beacons on every channel). Which, in-turn, allows the STA to make more efficient use of the air time and reduce its power consumption.

802.11v Wireless Network Management

MarQuest Networking Support

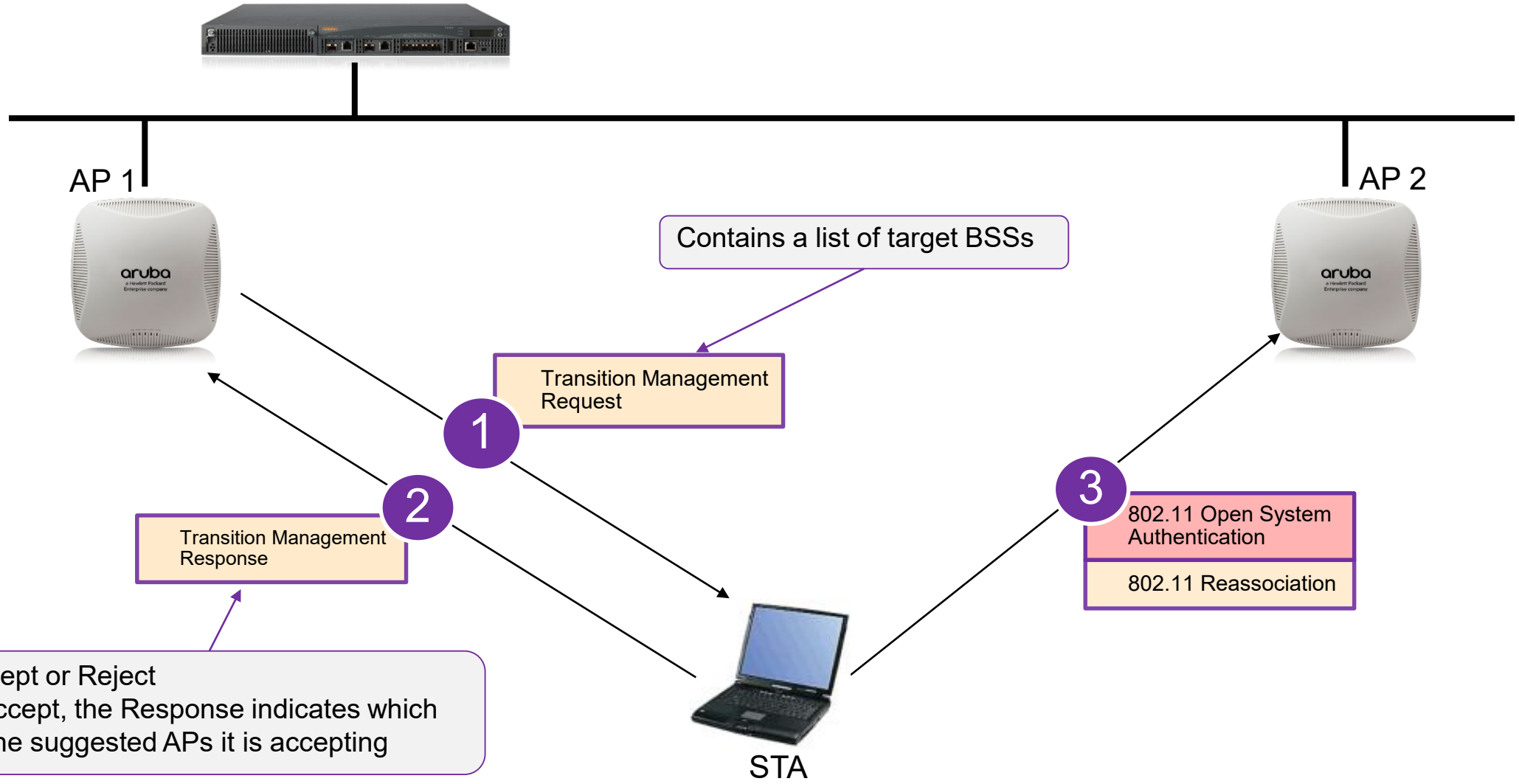
BSS Transition:
Used by the wireless infrastructure to request a client moves to a more appropriate AP within an ESS



802.11r Support:
Although some clients advertise support for 802.11v, they may not fully support BSS Transition.
Client vendors don't want to give up control to the wireless infrastructure.
Windows 10 supports BSS Transition with a supported adaptor and driver that also supports 802.11r

STAs use the Extended Capabilities element to advertise their support for BSS Transition

BSS Transition



BSS Transition Request Decode

MarQuest Networking Support

```
802.11 Management - Action
   Category Code:          10  WNM
   Action Code:            7  BSS Transition Management Request
   Dialog Token:           7
   Request mode:           %00000101
      Reserved:               %000
      ESS Disassociation Imminent:%0
      BSS Termination Included:%0
      Disassociation Imminent:%1
      Abridged:               %0
      Preferred Candidate List Included:%1
   Disassociation Timer: 1953
   Validity Interval:    200
   Neighbor Report
      Element ID:             52
      Length:                 16
      BSSID:                  74:A0:2F:B8:1E:7D
      BSSID Information:      %00000000000000000000001011110111
                                 ........ ........ ........ ..... 11 AP Reachability: Reachable (3)
                                 ........ ........ ........ .....1.. Security: the AP with this BSSID supports the same security provisioning as used by the STA
                                 ........ ........ ........ ....0... Key Scope: distinct authenticator or the information is not available
         Capabilities:           %00000000000000000000001011110000
                                    ........ ........ ........ ...1.... Spectrum Management: true
                                    ........ ........ ........ ..1..... QoS: true
                                    ........ ........ ........ .1...... APSD: true
                                    ........ ........ ........ 1....... Radio Measurement: true
                                    ........ ........ .......0 ........ Delayed Block Ack: false
                                    ........ ........ ......1. ........ Immediate Block Ack: true
                                 ........ ........ .....0.. ........ Mobility Domain: false
                                 ........ ........ ....0... ........ High Throughput: false
                                 xxxxxxxx xxxxxxxx ........ ........ Reserved: true
      Regulatory Class:       0
      Channel Number:         36
      PHY Type:               7
      Padding:                (3 bytes)
   Neighbor ReportElement ID=52Length=16 BSSID=88:1D:FC:6A:BA:0D BSSID Information=%00000000000000000000001011110111 Regulatory Class=0 Channel Number=48 PHY Type=7 Padding=(3 bytes)
   Neighbor ReportElement ID=52Length=16 BSSID=F0:7F:06:4D:C6:7D BSSID Information=%00000000000000000000001011110111 Regulatory Class=0 Channel Number=149 PHY Type=7 Padding=(3 bytes)
```

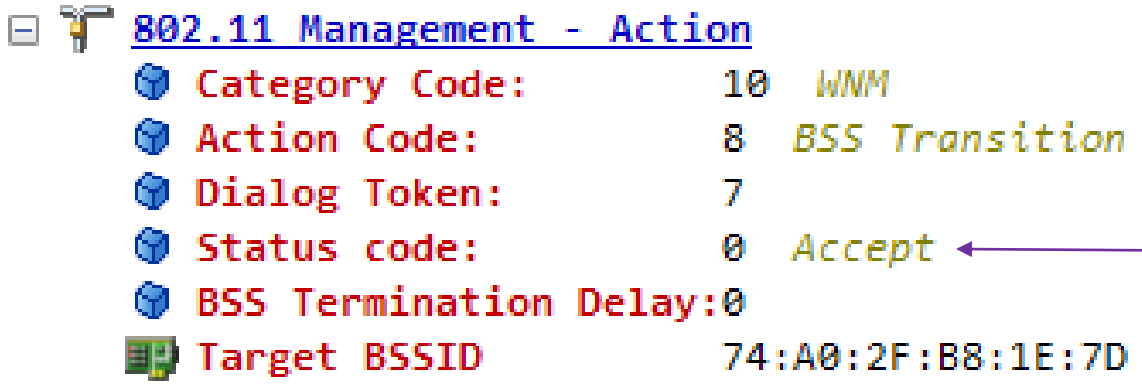
Number of TBTT until the AP sends a Disassociation frame to the STA

Neighbor's BSSID

Neighbor's Channel number

Additional Neighbor reports

BSS Transition Response Decode



Status Code accepted or rejected with one of 8 status codes

Status Code	Description
0	Accept
1	Reject—Unspecified reject reason.
2	Reject—Insufficient Beacon or Probe Response frames received from all candidates
3	Reject—Insufficient available capacity from all candidates
4	Reject—BSS termination undesired
5	Reject—BSS termination delay requested
6	Reject—STA BSS Transition Candidate List provided
7	Reject—No suitable BSS transition candidates
8	Reject—Leaving ESS
9-255	Reserved

What should we use?

MarQuest Networking Support

802.11r?

802.11k?

802.11v?