Analysis of a Fast Roam

Karsten Iwen

About Me

Karsten Iwen

- Freelance Consultant/Trainer

- 𝕏 @KarstenIwen
- www.linkedin.com/in/karsteniwen/
- 🌐 www.iwen.de
- 🌐 cyber-fi.net (Blog)

CISCO CERTIFIED CCIE SECURITY

CISCO CERTIFIED CCNP WIRELESS

CERTIFIED INFORMATION SYSTEMS SECURITY PROFESSIONAL CISSP

HAMINA WIRELESS CERTIFIED NETWORK ARCHITECT

ecse DESIGN

CERTIFIED Juniper JNCIS-MistAI SPECIALIST

CWSP Certified Wireless Security Professional

CWAP Certified Wireless Analysis Professional

CWDP Certified Wireless Design Professional

CWISA Certified Wireless IoT Solutions Administrator

CWNT Certified Wireless Network Trainer

What is a Roam?

basic service set (BSS) transition: Change of association by a station (STA) from one BSS to another BSS in the same extended service set (ESS).

pre-Auth - SKC - OKC
802.11r - Fast BSS Transition (2008)

fast basic service set (BSS) transition: Change of association by a station (STA) that is from one BSS in one extended service set (ESS) to another BSS in the same ESS and **that minimizes the amount of time that the data connectivity is lost between the STA and the distribution system (DS)**.

Disclaimer

Wi-Fi Checklist

Site _____

Date ___ / ___ / ___

wirelessLAN PROFESSIONALS

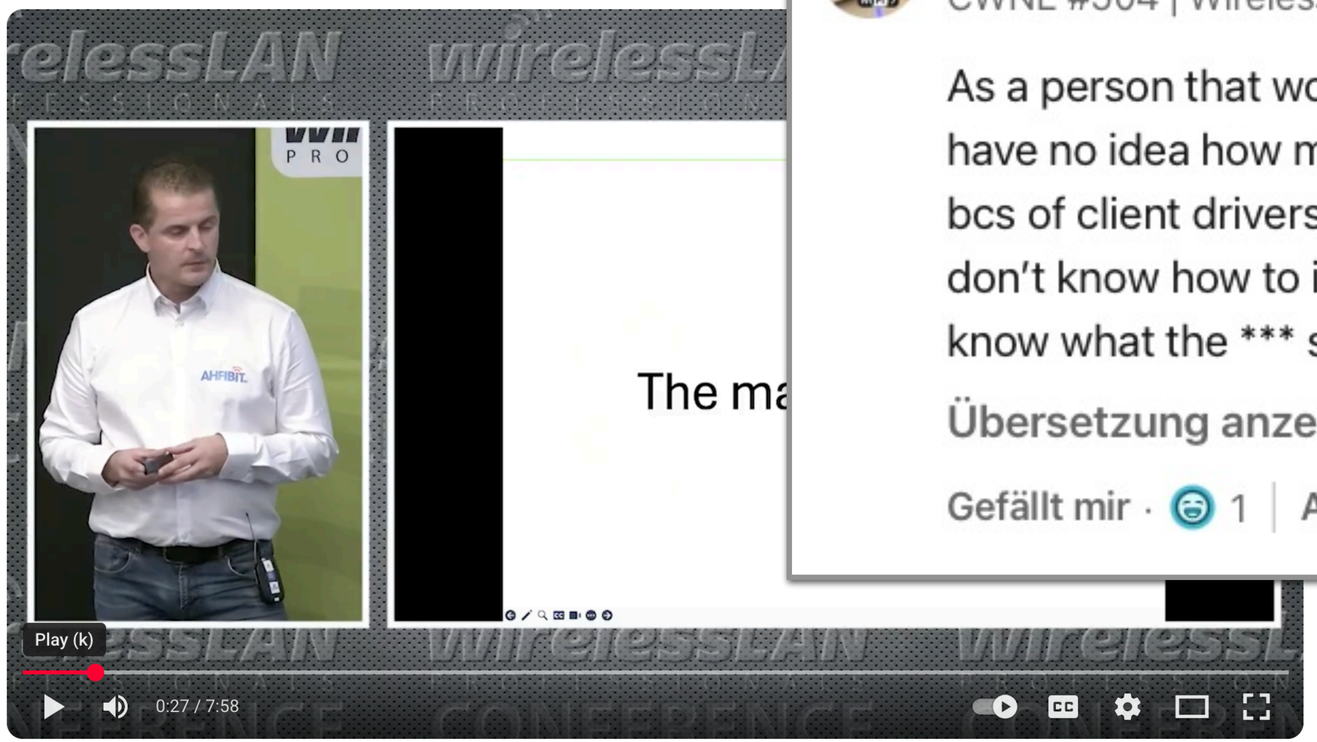
V.5 - 12 MAR - © 2024 WLAN Pros

Checklist to be used to quickly evaluate a Wi-Fi installation to a level of best practices. There will ALWA
situations where different metrics should be used. Please update green boxes for variable metrics for yo
requirements - Enter a 1 in the box

Notes

^^ - indicates some discussion in the community

	Items to Review and Report
1	1, 6, 11 Only
2	20 MHz Channels
3	40 MHz Channels
4	80 MHz Channels
5	802.11 b (HR) - Rates Disabled
6	802.11 k - Neighbor Report
7	802.11 r - Fast Transition *^*
8	802.11 v - Steering

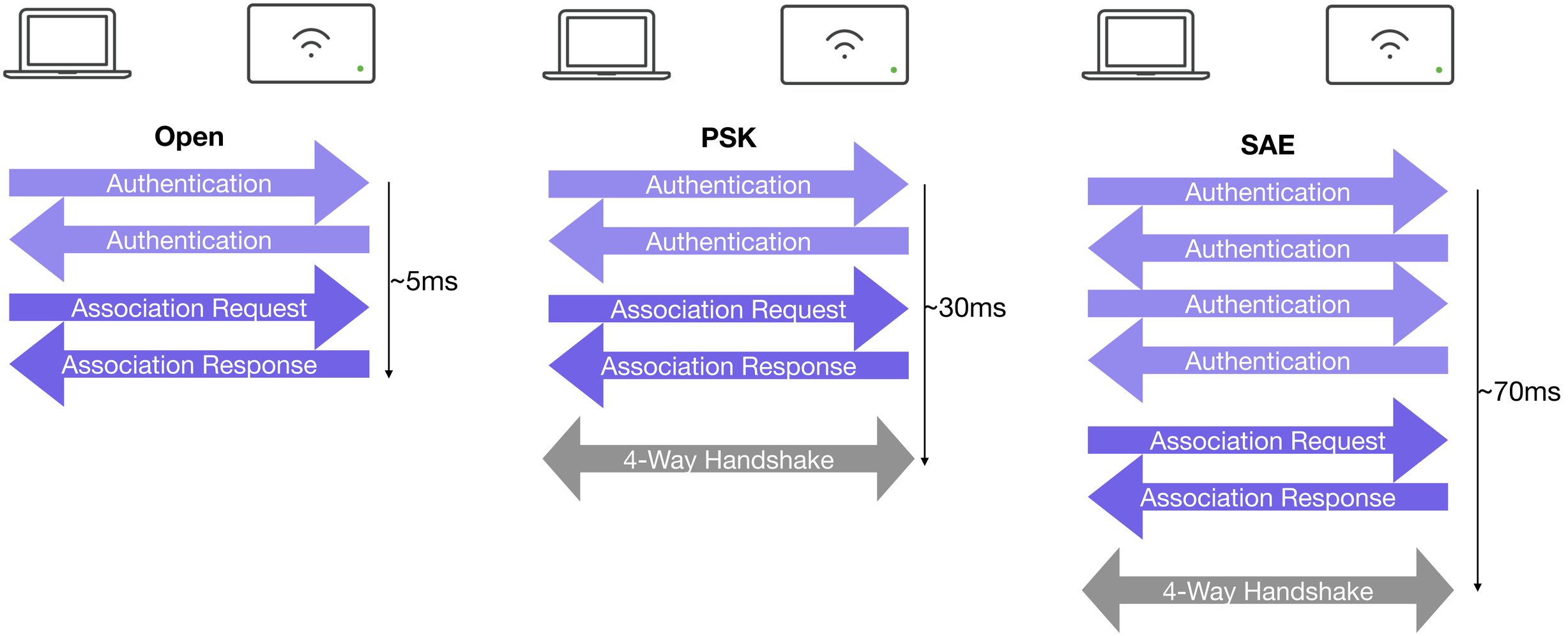


The Magical Roam | Hans Van Ballaer | WLPC Prague 2024

Some help to become „Fast“!

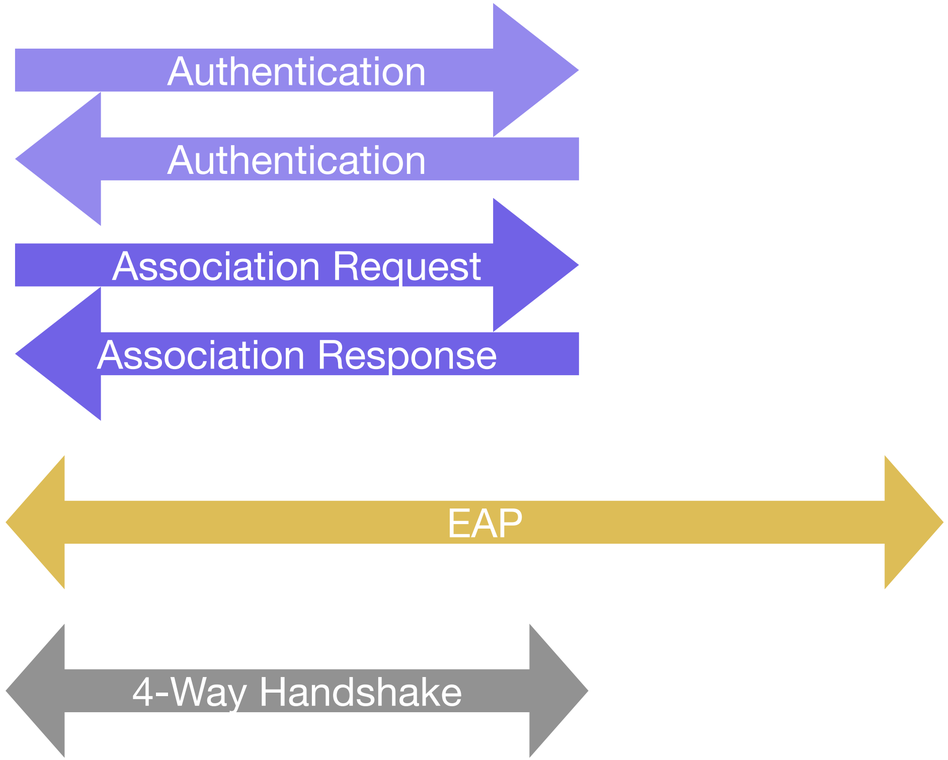
802.11k?
802.11v?
RNR?

„Fast“ enough?

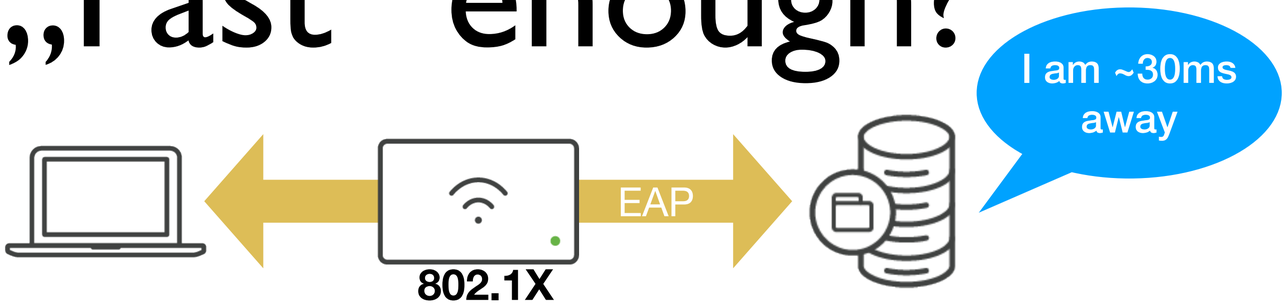

Open
Authentication
Authentication
Association Request
Association Response
~5ms
PSK
Authentication
Authentication
Association Request
Association Response
4-Way Handshake
~30ms
SAE
Authentication
Authentication
Authentication
Authentication
Association Request
Association Response
4-Way Handshake
~70ms

„Fast“ enough?

802.1X



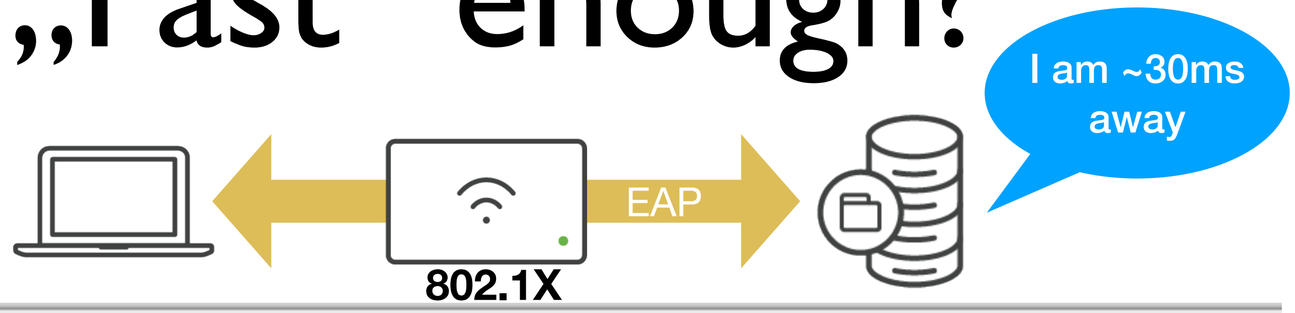
„Fast“ enough?



~300 ms

EAP	Info
Request	Request, Identity
Response	Response, Identity
Request	Request, TLS EAP (EAP-TLS)
Response	Client Hello
Request	Request, TLS EAP (EAP-TLS)
Response	Response, TLS EAP (EAP-TLS)
Request	Server Hello, Certificate, Server Key Exchange, Certificate Request, Server Hello Done
Response	Certificate, Client Key Exchange, Certificate Verify, Change Cipher Spec, Encrypted Handshake Message
Request	Change Cipher Spec, Encrypted Handshake Message
Response	Response, TLS EAP (EAP-TLS)
Success	Success

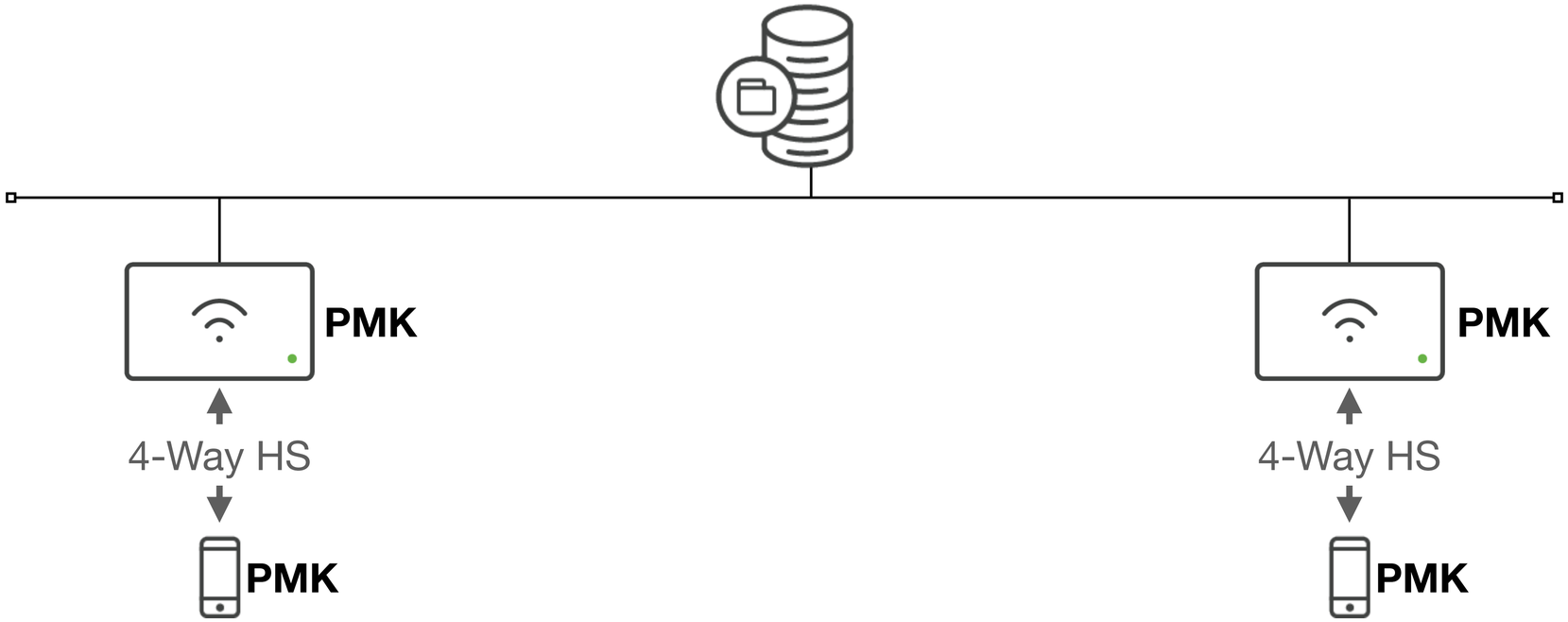
„Fast“ enough?



~500 ms

EAP	Info
Request	Request, Identity
Response	Response, Identity
Request	Request, TLS EAP (EAP-TLS)
Response	Response, Legacy Nak (Response Only)
Request	Request, Protected EAP (EAP-PEAP)
Response	Client Hello
Request	Request, Protected EAP (EAP-PEAP)
Response	Response, Protected EAP (EAP-PEAP)
Request	Server Hello, Certificate, Server Key Exchange, Server Hello Done
Response	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
Request	Change Cipher Spec, Encrypted Handshake Message
Response	Response, Protected EAP (EAP-PEAP)
Request	Application Data
Response	Application Data
Request	Application Data
Response	Application Data
Request	Application Data
Response	Application Data
Request	Application Data
Response	Response, Protected EAP (EAP-PEAP)
Success	Success

Fast BSS Transition

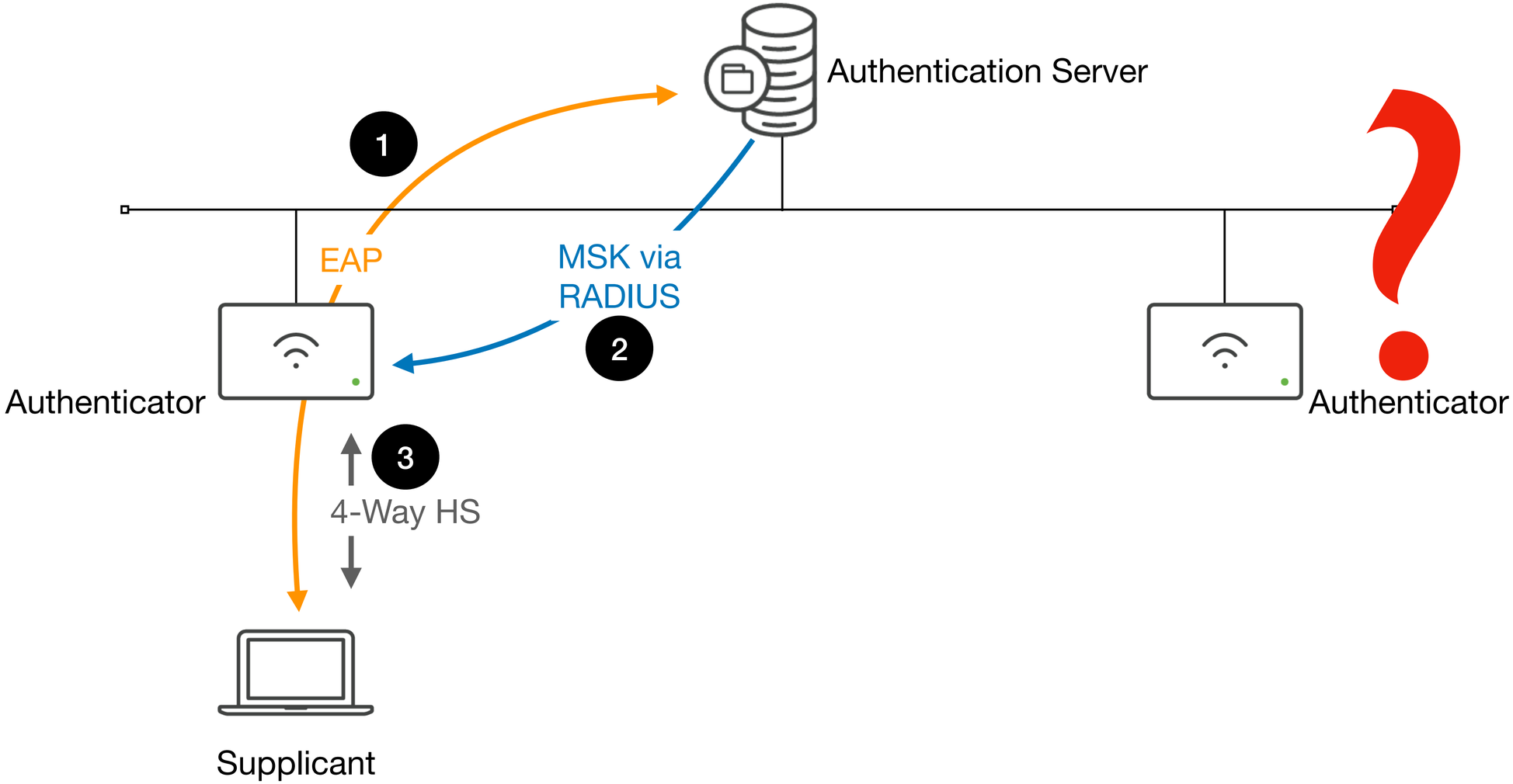


Assumptions:

- Each STA-AP combination needs a 4-Way-Handshake generate the PTK from the PMK.

- Each STA-AP combination needs a PMK.

Fast BSS Transition



Key Hierarchy

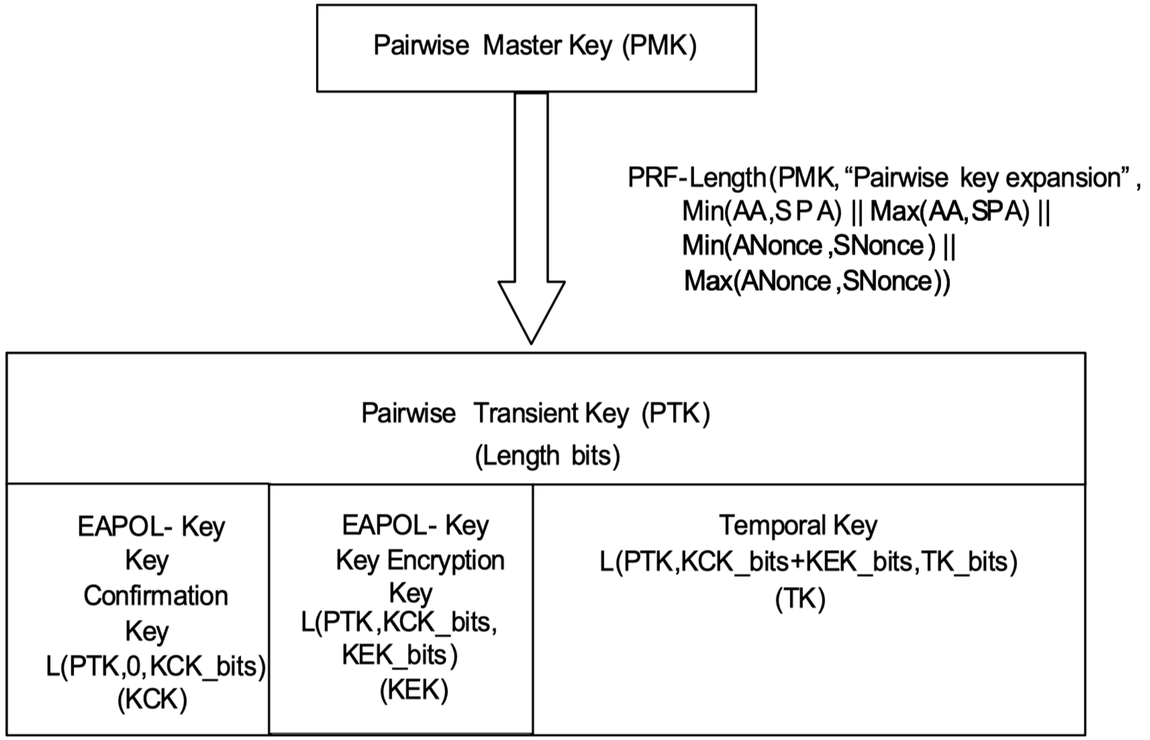


Figure 12-30—Pairwise key hierarchy

Key Hierarchy

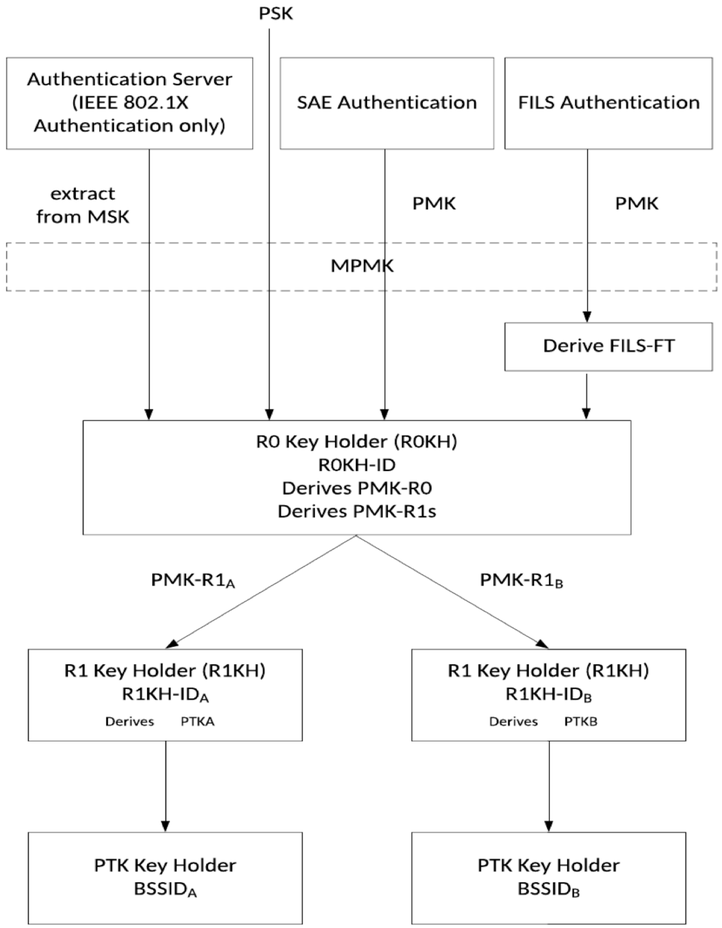
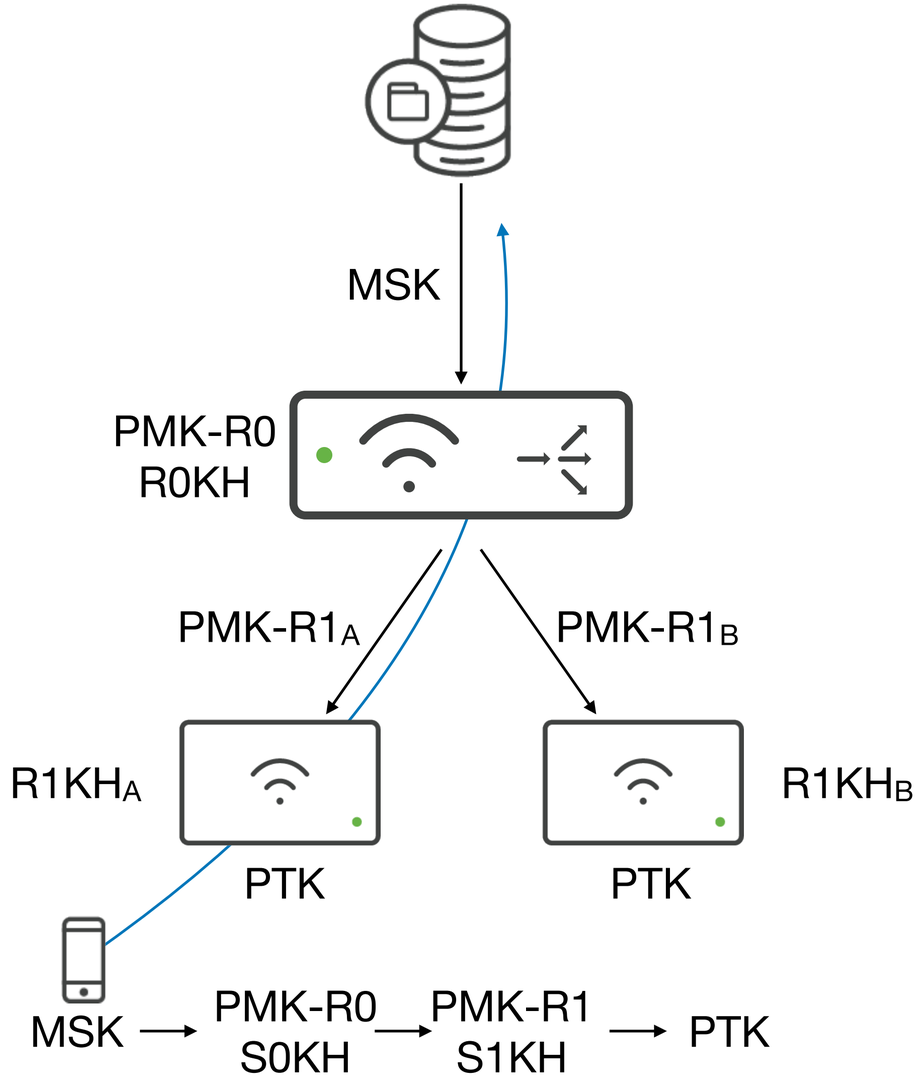
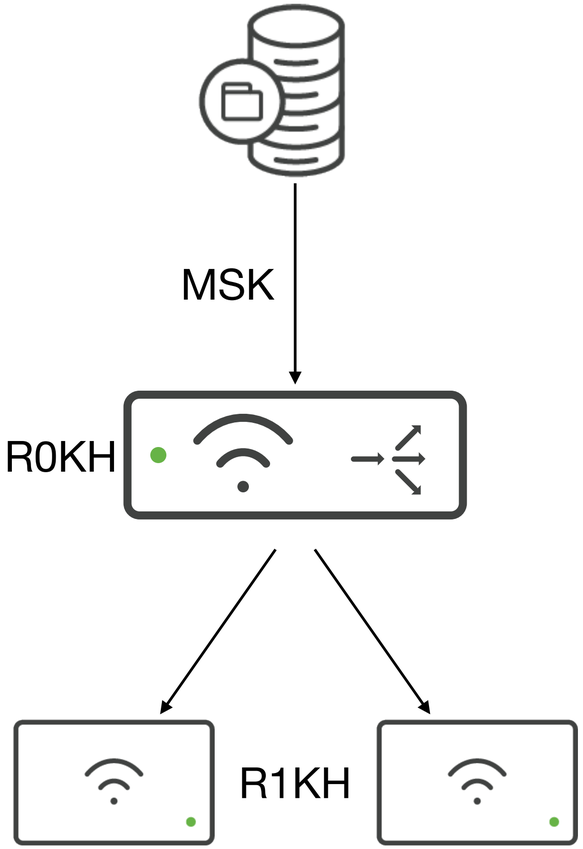


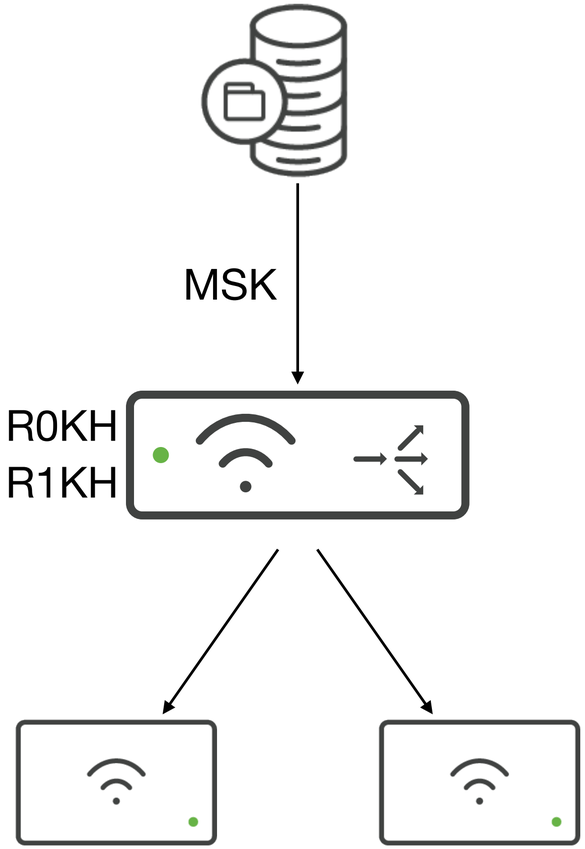
Figure 12-32—FT key hierarchy at an Authenticator

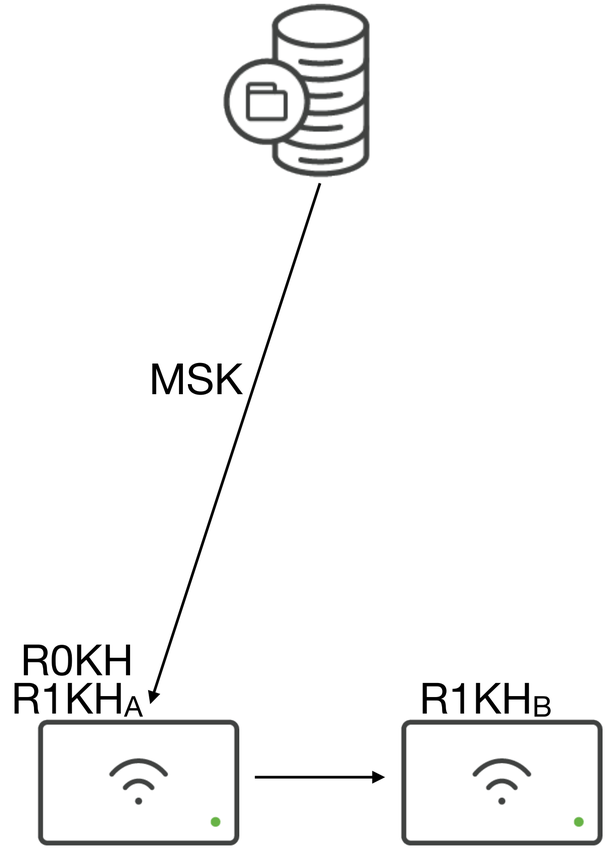
IEEE Std 802.11-2020



Key Hierarchy







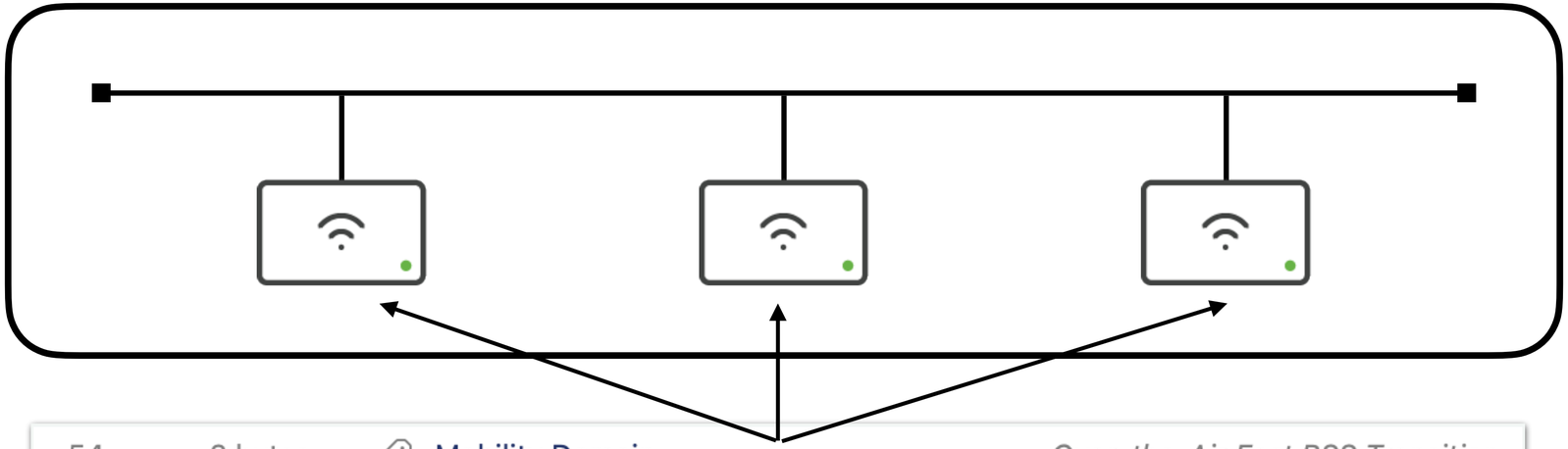
The R0KH interacts with the IEEE 802.1X Authenticator to receive the MSK resulting from an EAP authentication.
The R1KH interacts with the IEEE 802.1X Authenticator to open the Controlled Port.

Is Fast BSS Transition available?

mobility domain: A set of basic service sets (BSSs), within the same extended service set (ESS), that support fast BSS transitions between themselves and that are identified by the set's mobility domain identifier (MDID).

mobility domain identifier (MDID): An identifier that names a mobility domain.

Is Fast BSS Transition available?



54	3 bytes	Mobility Domain	*Over-the-Air Fast BSS Transition*
		Element ID:	54
		Length:	3 bytes
		MDID:	13484 0x34ac
		FT Capability and Policy:	0x00

	Element ID	Length	MDID	FT Capability and Policy
Octets:	1	1	2	1

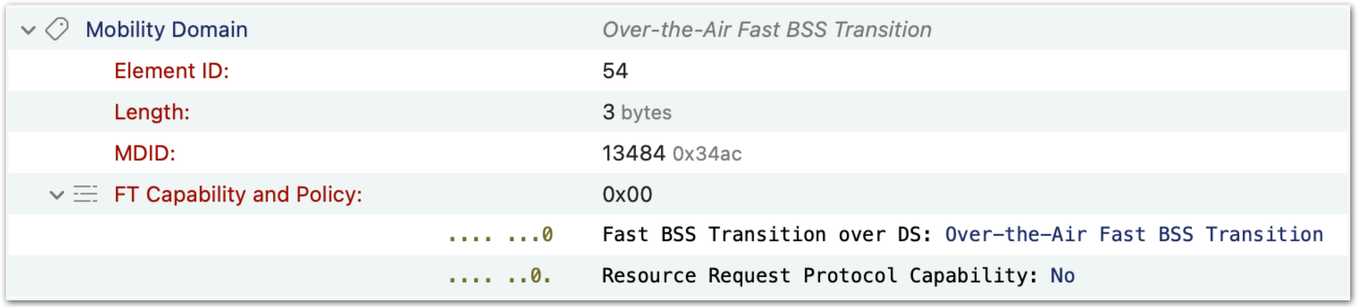
Figure 9-354—Mobility Domain element format

	B0	B1	B2	B7
	Fast BSS Transition over DS	Resource Request Protocol Capability	Reserved	
Bits:	1	1	6	

Figure 9-355—FT Capability and Policy field format

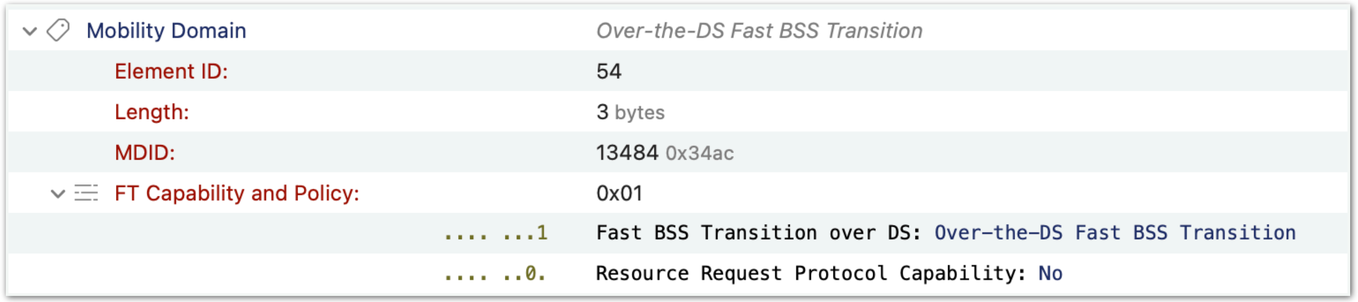
Is Fast BSS Transition available?

- **Two modes**
  - **Over-the-Air**



Mobility Domain		*Over-the-Air Fast BSS Transition*
Element ID:		54
Length:		3 bytes
MDID:		13484 0x34ac
FT Capability and Policy:		0x00
	0	Fast BSS Transition over DS: Over-the-Air Fast BSS Transition
	.... ..0.	Resource Request Protocol Capability: No

  - **Over-the-DS**

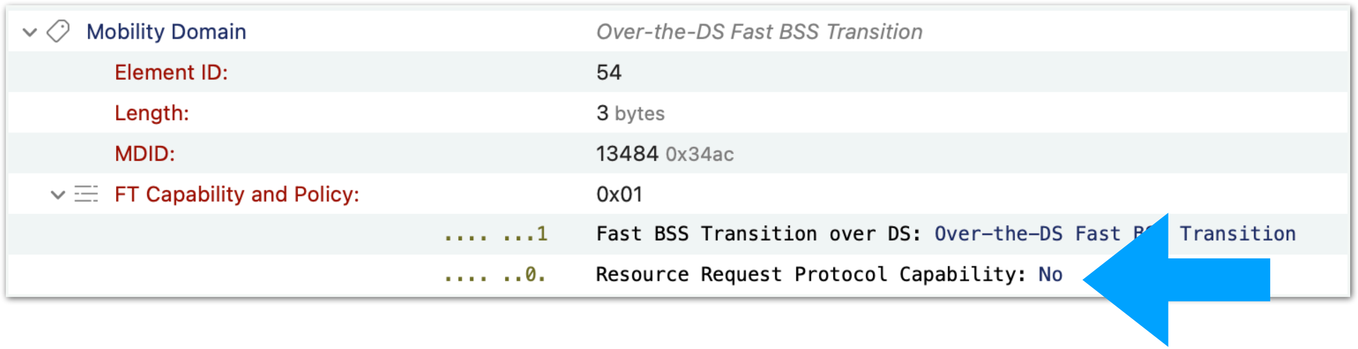


Mobility Domain		*Over-the-DS Fast BSS Transition*
Element ID:		54
Length:		3 bytes
MDID:		13484 0x34ac
FT Capability and Policy:		0x01
	1	Fast BSS Transition over DS: Over-the-DS Fast BSS Transition
	.... ..0.	Resource Request Protocol Capability: No

Is Fast BSS Transition available?

- **Two protocols**
  - **FT protocol**
  - **FT resource request protocol**
    This protocol is executed when an FTO requires a resource request prior to its transition.

FT Originator (the STA)



Is Fast BSS Transition available?

Table 9-151—AKM suite selectors

OUI	Suite type	Meaning			Authentication algorithm numbers (see 9.4.1.1)
		Authentication type	Key management type	Key derivation type	
00-0F-AC	0	Reserved	Reserved	Reserved	Reserved
00-0F-AC	1	Authentication negotiated over IEEE Std 802.1X	RSNA key management as defined in 12.7	Defined in 12.7.1.2	0 (open)
00-0F-AC	2	PSK	RSNA key management as defined in 12.7	Defined in 12.7.1.2	0 (open)

non-FT

Table 9-151—AKM suite selectors

OUI	Suite type	Meaning			Authentication algorithm numbers (see 9.4.1.1)
		Authentication type	Key management type	Key derivation type	
00-0F-AC	3	FT authentication negotiated over IEEE Std 802.1X	FT key management as defined in 12.7.1.6	Defined in 12.7.1.6.2 using SHA-256	2 (FT) for FT protocol reassociation as defined in 13.5 0 (open) for FT Initial Mobility Domain Association over IEEE Std 802.1X or PMKSA caching
00-0F-AC	4	FT authentication using PSK	FT key management as defined in 12.7.1.6	Defined in 12.7.1.6.2 using SHA-256	2 (FT) for FT protocol reassociation as defined in 13.5 0 (open) for FT Initial Mobility Domain Association using PSK

FT

9.4.2.24.3 AKM suites

Is Fast BSS Transition available?

RSNE	*Group Cipher: CCMP-128; Pairwise*
Element ID:	48
Length:	26 bytes
Version:	1
Group Cipher Suite OUI:	00-0F-AC (IEEE 802.11)
Group Cipher Suite Type:	CCMP-128 (4)
Pairwise Cipher Suite Count:	1
Pairwise Cipher Suite List	
Auth Key Management Suite Count:	1
Auth Key Management Suite List	
Auth Key Management Suite OUI:	00-0F-AC (IEEE 802.11)
Auth Key Management Suite Type:	FT-802.1X (3)

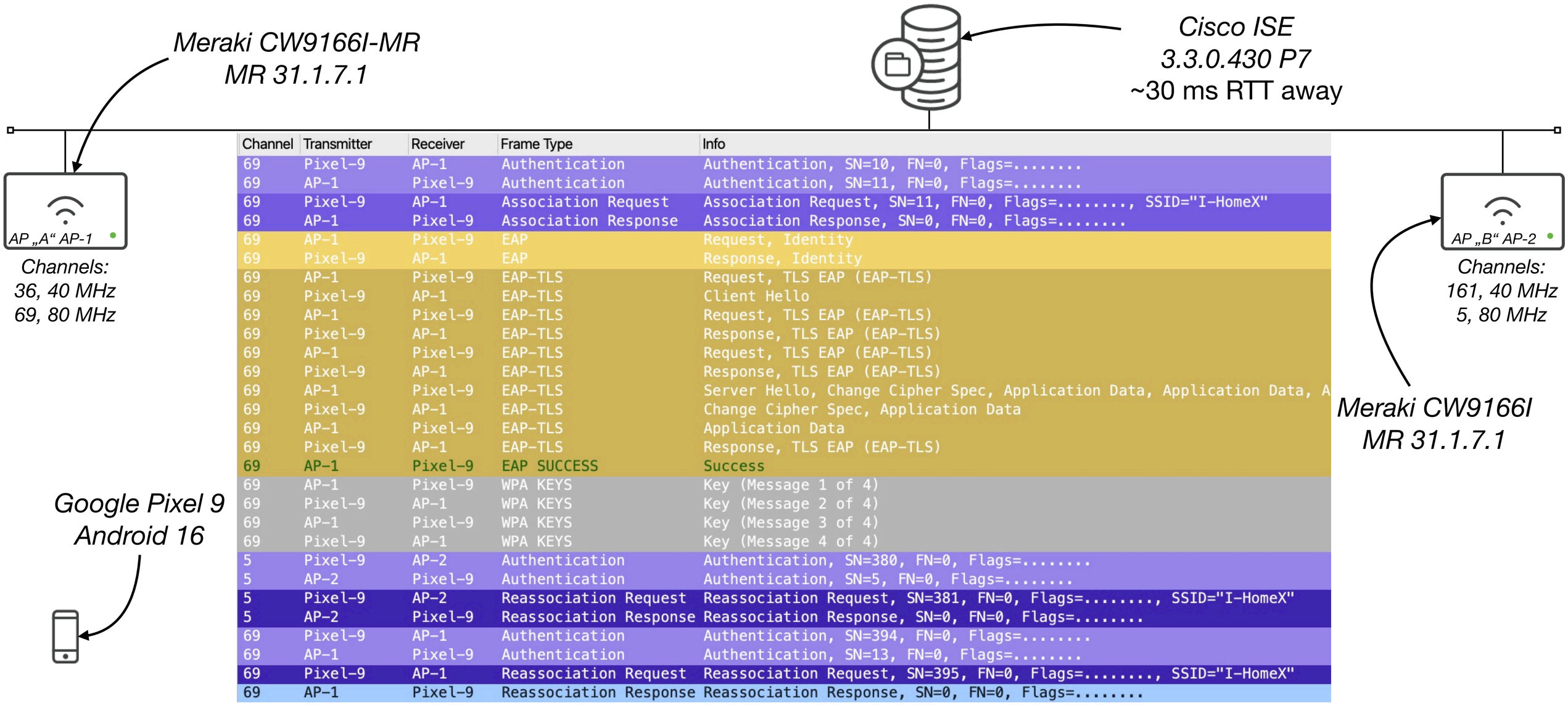
RSNE	*Group Cipher: CCMP-128; Pairwise*
Element ID:	48
Length:	30 bytes
Version:	1
Group Cipher Suite OUI:	00-0F-AC (IEEE 802.11)
Group Cipher Suite Type:	CCMP-128 (4)
Pairwise Cipher Suite Count:	1
Pairwise Cipher Suite List	
Auth Key Management Suite Count:	2
Auth Key Management Suite List	
Auth Key Management Suite OUI:	00-0F-AC (IEEE 802.11)
Auth Key Management Suite Type:	FT-802.1X (3)
Auth Key Management Suite OUI:	00-0F-AC (IEEE 802.11)
Auth Key Management Suite Type:	802.1X (SHA-256) (5)

Is Fast BSS Transition available?

RSNE	*Group Cipher: CCMP-128; Pairwise*
Element ID:	48
Length:	26 bytes
Version:	1
Group Cipher Suite OUI:	00-0F-AC (IEEE 802.11)
Group Cipher Suite Type:	CCMP-128 (4)
Pairwise Cipher Suite Count:	1
Pairwise Cipher Suite List	
Auth Key Management Suite Count:	1
Auth Key Management Suite List	
Auth Key Management Suite OUI:	00-0F-AC (IEEE 802.11)
Auth Key Management Suite Type:	802.1X (1)

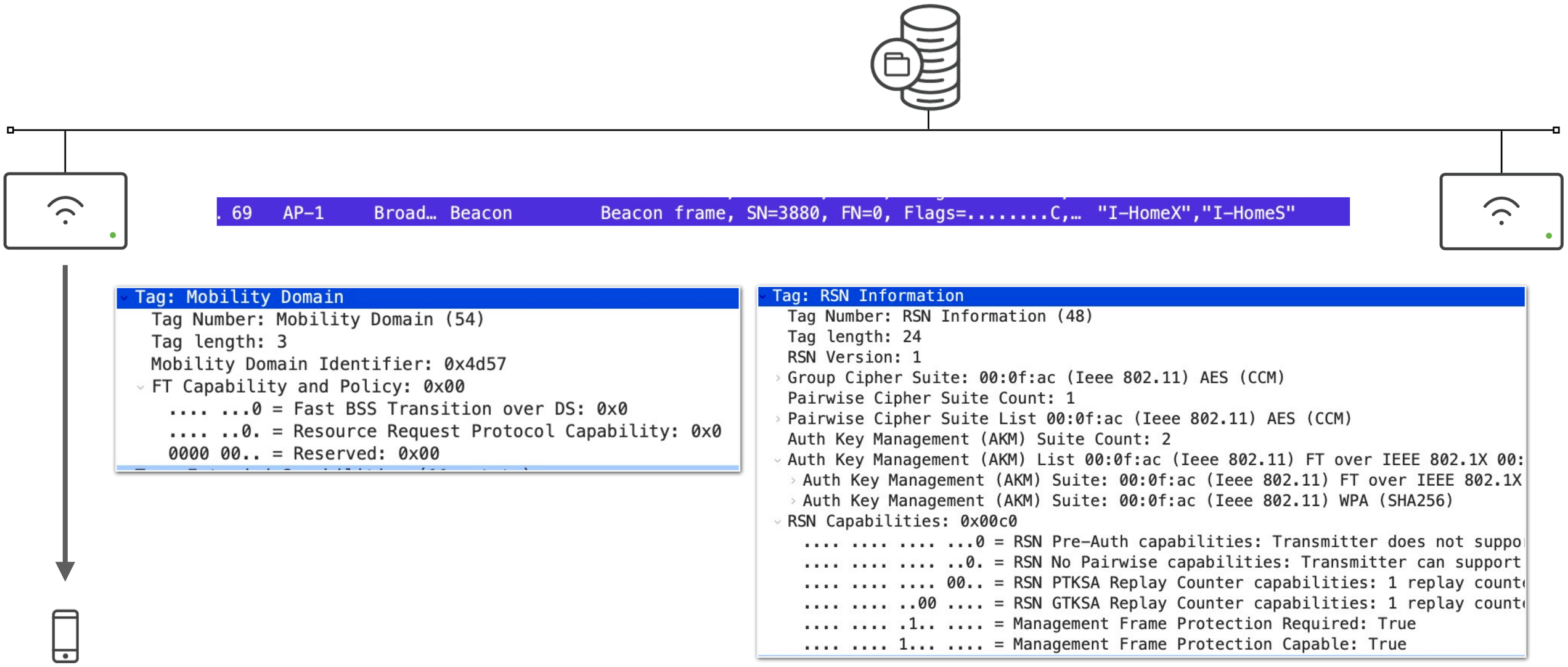
Mobility Domain	*Over-the-Air Fast BSS Transition*
Element ID:	54
Length:	3 bytes
MDID:	13484 0x34ac
FT Capability and Policy:	0x00

Frame by Frame



Channel	Transmitter	Receiver	Frame Type	Info
69	Pixel-9	AP-1	Authentication	Authentication, SN=10, FN=0, Flags=........
69	AP-1	Pixel-9	Authentication	Authentication, SN=11, FN=0, Flags=........
69	Pixel-9	AP-1	Association Request	Association Request, SN=11, FN=0, Flags=........, SSID="I-HomeX"
69	AP-1	Pixel-9	Association Response	Association Response, SN=0, FN=0, Flags=........
69	AP-1	Pixel-9	EAP	Request, Identity
69	Pixel-9	AP-1	EAP	Response, Identity
69	AP-1	Pixel-9	EAP-TLS	Request, TLS EAP (EAP-TLS)
69	Pixel-9	AP-1	EAP-TLS	Client Hello
69	AP-1	Pixel-9	EAP-TLS	Request, TLS EAP (EAP-TLS)
69	Pixel-9	AP-1	EAP-TLS	Response, TLS EAP (EAP-TLS)
69	AP-1	Pixel-9	EAP-TLS	Request, TLS EAP (EAP-TLS)
69	Pixel-9	AP-1	EAP-TLS	Response, TLS EAP (EAP-TLS)
69	AP-1	Pixel-9	EAP-TLS	Server Hello, Change Cipher Spec, Application Data, Application Data, A
69	Pixel-9	AP-1	EAP-TLS	Change Cipher Spec, Application Data
69	AP-1	Pixel-9	EAP-TLS	Application Data
69	Pixel-9	AP-1	EAP-TLS	Response, TLS EAP (EAP-TLS)
69	AP-1	Pixel-9	EAP SUCCESS	Success
69	AP-1	Pixel-9	WPA KEYS	Key (Message 1 of 4)
69	Pixel-9	AP-1	WPA KEYS	Key (Message 2 of 4)
69	AP-1	Pixel-9	WPA KEYS	Key (Message 3 of 4)
69	Pixel-9	AP-1	WPA KEYS	Key (Message 4 of 4)
5	Pixel-9	AP-2	Authentication	Authentication, SN=380, FN=0, Flags=........
5	AP-2	Pixel-9	Authentication	Authentication, SN=5, FN=0, Flags=........
5	Pixel-9	AP-2	Reassociation Request	Reassociation Request, SN=381, FN=0, Flags=........, SSID="I-HomeX"
5	AP-2	Pixel-9	Reassociation Response	Reassociation Response, SN=0, FN=0, Flags=........
69	Pixel-9	AP-1	Authentication	Authentication, SN=394, FN=0, Flags=........
69	AP-1	Pixel-9	Authentication	Authentication, SN=13, FN=0, Flags=........
69	Pixel-9	AP-1	Reassociation Request	Reassociation Request, SN=395, FN=0, Flags=........, SSID="I-HomeX"
69	AP-1	Pixel-9	Reassociation Response	Reassociation Response, SN=0, FN=0, Flags=........

Frame by Frame

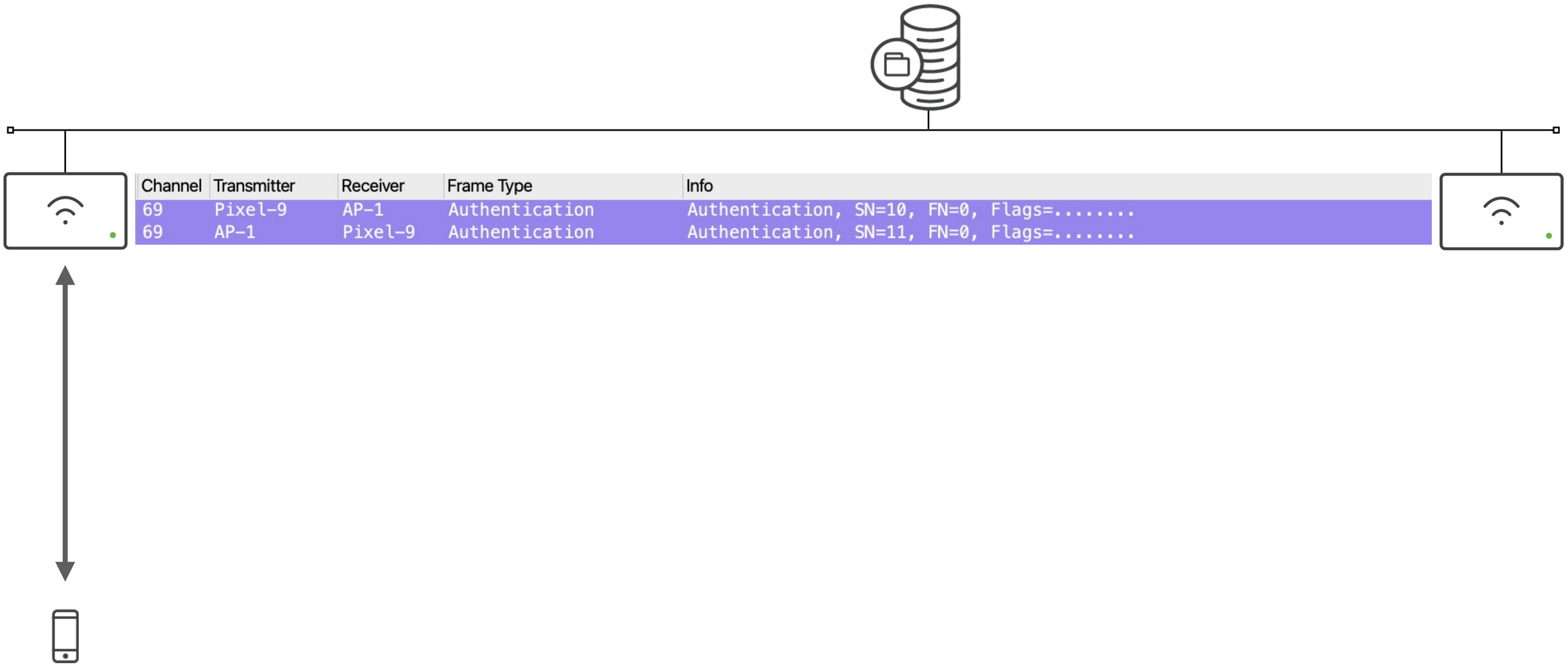


```
. 69   AP-1     Broad… Beacon        Beacon frame, SN=3880, FN=0, Flags=........C,…  "I-HomeX","I-HomeS"
```

```
Tag: Mobility Domain
  Tag Number: Mobility Domain (54)
  Tag length: 3
  Mobility Domain Identifier: 0x4d57
  FT Capability and Policy: 0x00
    .... ...0 = Fast BSS Transition over DS: 0x0
    .... ..0. = Resource Request Protocol Capability: 0x0
    0000 00.. = Reserved: 0x00
```

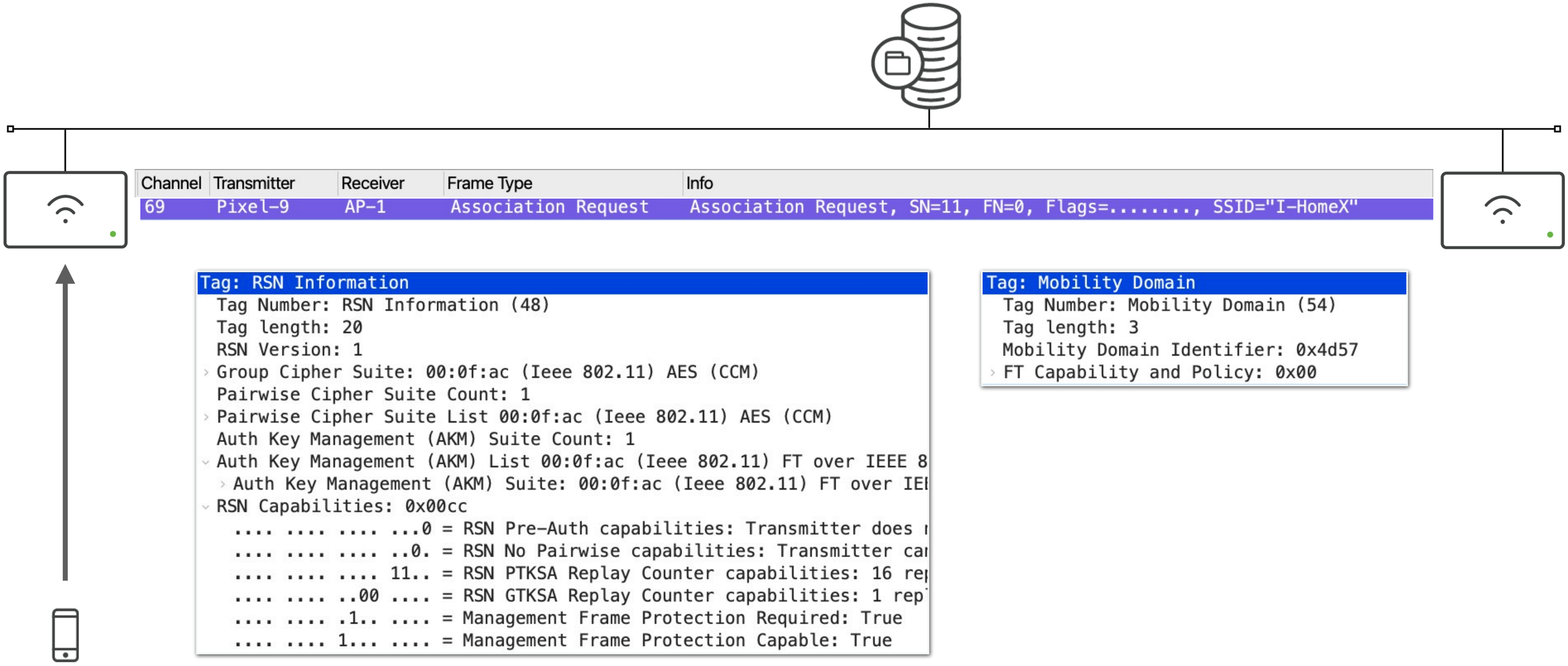
```
Tag: RSN Information
  Tag Number: RSN Information (48)
  Tag length: 24
  RSN Version: 1
  Group Cipher Suite: 00:0f:ac (Ieee 802.11) AES (CCM)
  Pairwise Cipher Suite Count: 1
  Pairwise Cipher Suite List 00:0f:ac (Ieee 802.11) AES (CCM)
  Auth Key Management (AKM) Suite Count: 2
  Auth Key Management (AKM) List 00:0f:ac (Ieee 802.11) FT over IEEE 802.1X 00:
    Auth Key Management (AKM) Suite: 00:0f:ac (Ieee 802.11) FT over IEEE 802.1X
    Auth Key Management (AKM) Suite: 00:0f:ac (Ieee 802.11) WPA (SHA256)
  RSN Capabilities: 0x00c0
    .... .... .... ...0 = RSN Pre-Auth capabilities: Transmitter does not suppo
    .... .... .... ..0. = RSN No Pairwise capabilities: Transmitter can support
    .... .... .... 00.. = RSN PTKSA Replay Counter capabilities: 1 replay counte
    .... .... ..00 .... = RSN GTKSA Replay Counter capabilities: 1 replay counte
    .... .... .1.. .... = Management Frame Protection Required: True
    .... .... 1... .... = Management Frame Protection Capable: True
```

Frame by Frame



Channel	Transmitter	Receiver	Frame Type	Info
69	Pixel-9	AP-1	Authentication	Authentication, SN=10, FN=0, Flags=........
69	AP-1	Pixel-9	Authentication	Authentication, SN=11, FN=0, Flags=........

Frame by Frame

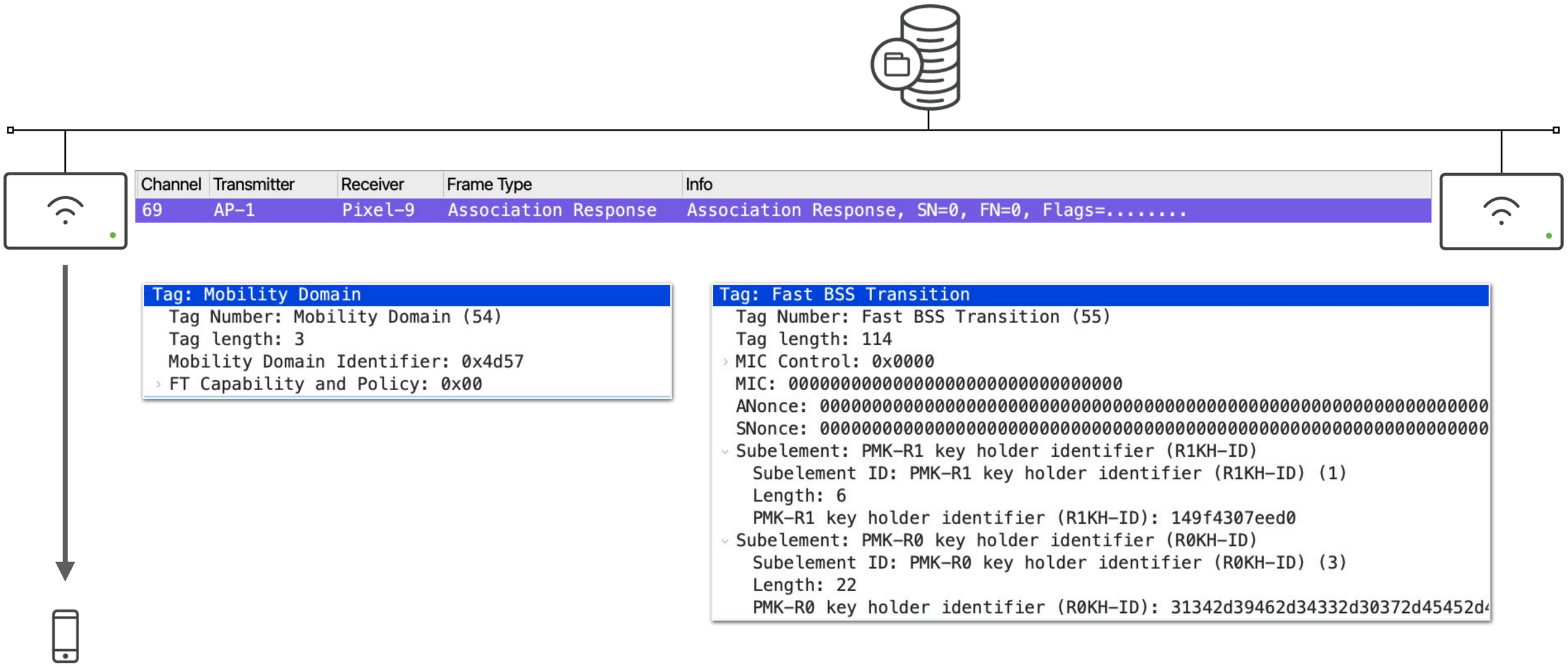


Channel	Transmitter	Receiver	Frame Type	Info
69	Pixel-9	AP-1	Association Request	Association Request, SN=11, FN=0, Flags=........, SSID="I-HomeX"

```
Tag: RSN Information
  Tag Number: RSN Information (48)
  Tag length: 20
  RSN Version: 1
› Group Cipher Suite: 00:0f:ac (Ieee 802.11) AES (CCM)
  Pairwise Cipher Suite Count: 1
› Pairwise Cipher Suite List 00:0f:ac (Ieee 802.11) AES (CCM)
  Auth Key Management (AKM) Suite Count: 1
⌄ Auth Key Management (AKM) List 00:0f:ac (Ieee 802.11) FT over IEEE 8
  › Auth Key Management (AKM) Suite: 00:0f:ac (Ieee 802.11) FT over IEE
⌄ RSN Capabilities: 0x00cc
    .... .... .... ...0 = RSN Pre-Auth capabilities: Transmitter does
    .... .... .... ..0. = RSN No Pairwise capabilities: Transmitter ca
    .... .... .... 11.. = RSN PTKSA Replay Counter capabilities: 16 re
    .... .... ..00 .... = RSN GTKSA Replay Counter capabilities: 1 rep
    .... .... .1.. .... = Management Frame Protection Required: True
    .... .... 1... .... = Management Frame Protection Capable: True
```

```
Tag: Mobility Domain
  Tag Number: Mobility Domain (54)
  Tag length: 3
  Mobility Domain Identifier: 0x4d57
› FT Capability and Policy: 0x00
```

Frame by Frame

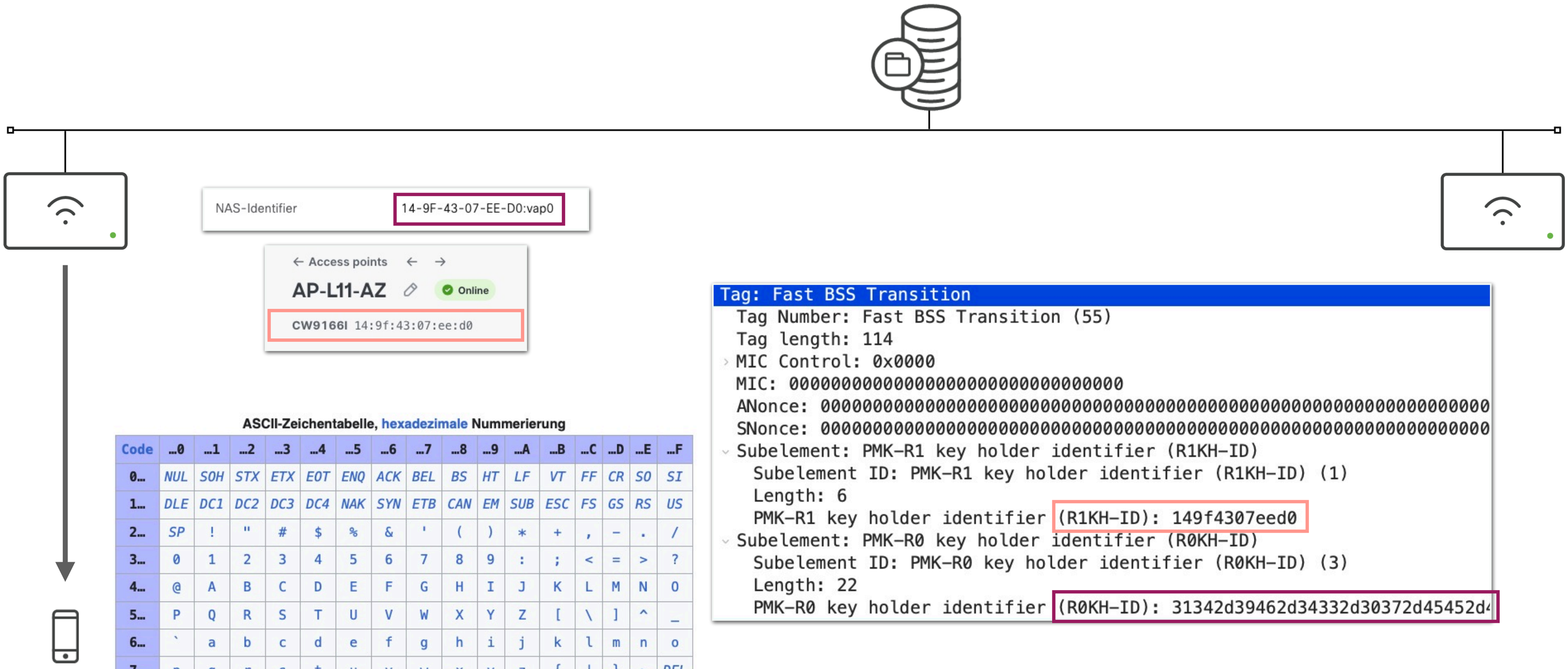


Channel	Transmitter	Receiver	Frame Type	Info
69	AP-1	Pixel-9	Association Response	Association Response, SN=0, FN=0, Flags=........

```
Tag: Mobility Domain
  Tag Number: Mobility Domain (54)
  Tag length: 3
  Mobility Domain Identifier: 0x4d57
› FT Capability and Policy: 0x00
```

```
Tag: Fast BSS Transition
  Tag Number: Fast BSS Transition (55)
  Tag length: 114
› MIC Control: 0x0000
  MIC: 00000000000000000000000000000000
  ANonce: 0000000000000000000000000000000000000000000000000000000000000000
  SNonce: 0000000000000000000000000000000000000000000000000000000000000000
⌄ Subelement: PMK-R1 key holder identifier (R1KH-ID)
    Subelement ID: PMK-R1 key holder identifier (R1KH-ID) (1)
    Length: 6
    PMK-R1 key holder identifier (R1KH-ID): 149f4307eed0
⌄ Subelement: PMK-R0 key holder identifier (R0KH-ID)
    Subelement ID: PMK-R0 key holder identifier (R0KH-ID) (3)
    Length: 22
    PMK-R0 key holder identifier (R0KH-ID): 31342d39462d34332d30372d45452d4
```

Frame by Frame



NAS-Identifier 14-9F-43-07-EE-D0:vap0

← Access points ← →

AP-L11-AZ Online

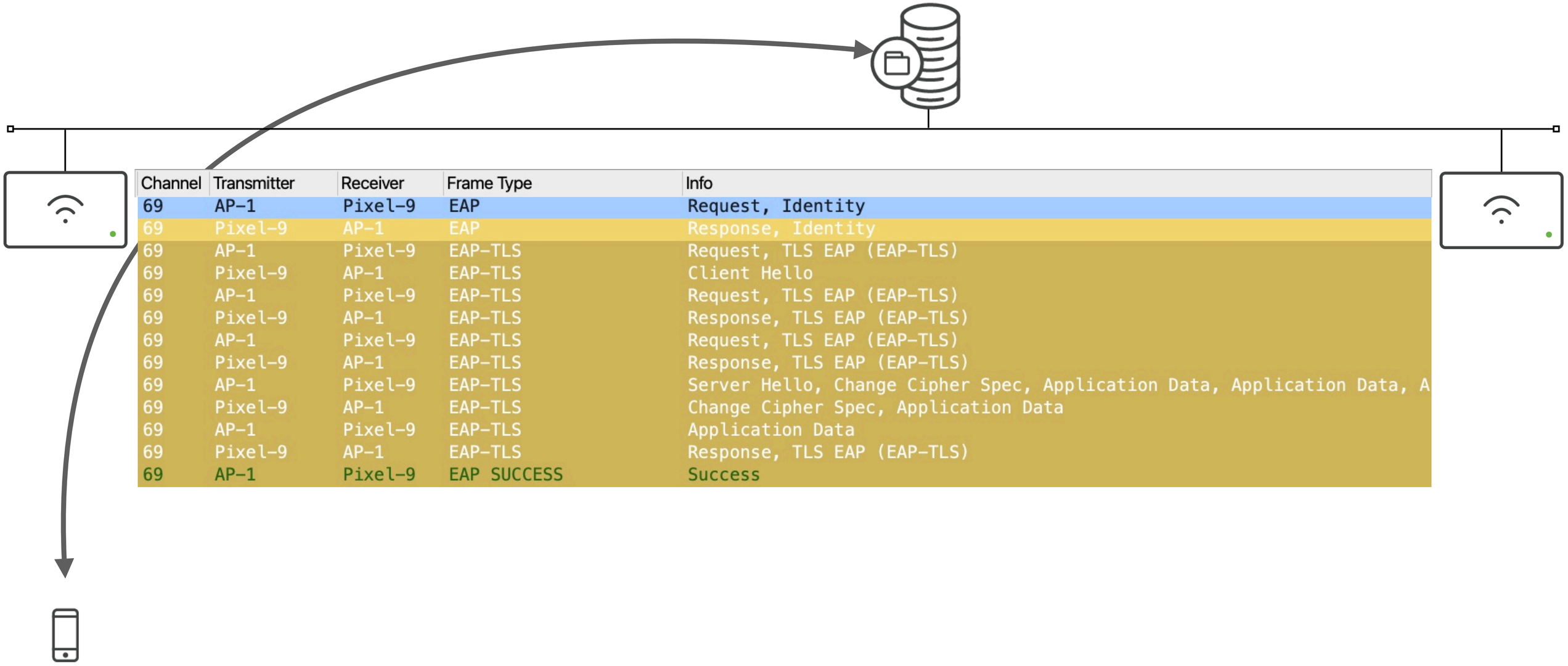
CW9166I 14:9f:43:07:ee:d0

ASCII-Zeichentabelle, hexadezimale Nummerierung

Code	…0	…1	…2	…3	…4	…5	…6	…7	…8	…9	…A	…B	…C	…D	…E	…F
0…	NUL	SOH	STX	ETX	EOT	ENQ	ACK	BEL	BS	HT	LF	VT	FF	CR	SO	SI
1…	DLE	DC1	DC2	DC3	DC4	NAK	SYN	ETB	CAN	EM	SUB	ESC	FS	GS	RS	US
2…	SP	!	"	#	$	%	&	'	(	)	*	+	,	-	.	/
3…	0	1	2	3	4	5	6	7	8	9	:	;	<	=	>	?
4…	@	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
5…	P	Q	R	S	T	U	V	W	X	Y	Z	[	\	]	^	_
6…	`	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o
7…	p	q	r	s	t	u	v	w	x	y	z	{	|	}	~	DEL

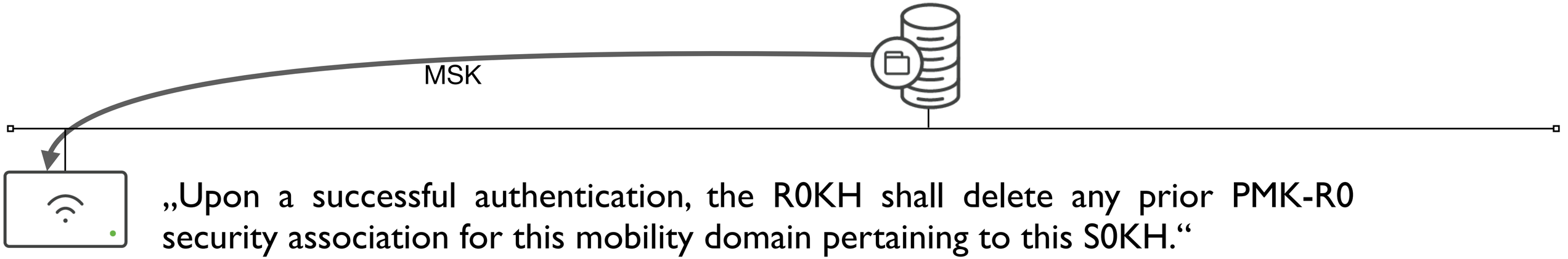
```
Tag: Fast BSS Transition
  Tag Number: Fast BSS Transition (55)
  Tag length: 114
› MIC Control: 0x0000
  MIC: 00000000000000000000000000000000
  ANonce: 0000000000000000000000000000000000000000000000000000000000000000
  SNonce: 0000000000000000000000000000000000000000000000000000000000000000
⌄ Subelement: PMK-R1 key holder identifier (R1KH-ID)
    Subelement ID: PMK-R1 key holder identifier (R1KH-ID) (1)
    Length: 6
    PMK-R1 key holder identifier (R1KH-ID): 149f4307eed0
⌄ Subelement: PMK-R0 key holder identifier (R0KH-ID)
    Subelement ID: PMK-R0 key holder identifier (R0KH-ID) (3)
    Length: 22
    PMK-R0 key holder identifier (R0KH-ID): 31342d39462d34332d30372d45452d4
```

Frame by Frame



Channel	Transmitter	Receiver	Frame Type	Info
69	AP-1	Pixel-9	EAP	Request, Identity
69	Pixel-9	AP-1	EAP	Response, Identity
69	AP-1	Pixel-9	EAP-TLS	Request, TLS EAP (EAP-TLS)
69	Pixel-9	AP-1	EAP-TLS	Client Hello
69	AP-1	Pixel-9	EAP-TLS	Request, TLS EAP (EAP-TLS)
69	Pixel-9	AP-1	EAP-TLS	Response, TLS EAP (EAP-TLS)
69	AP-1	Pixel-9	EAP-TLS	Request, TLS EAP (EAP-TLS)
69	Pixel-9	AP-1	EAP-TLS	Response, TLS EAP (EAP-TLS)
69	AP-1	Pixel-9	EAP-TLS	Server Hello, Change Cipher Spec, Application Data, Application Data, A
69	Pixel-9	AP-1	EAP-TLS	Change Cipher Spec, Application Data
69	AP-1	Pixel-9	EAP-TLS	Application Data
69	Pixel-9	AP-1	EAP-TLS	Response, TLS EAP (EAP-TLS)
69	AP-1	Pixel-9	EAP SUCCESS	Success

Frame by Frame



„Upon a successful authentication, the R0KH shall delete any prior PMK-R0 security association for this mobility domain pertaining to this S0KH.“

12.7.1.6.1 Overview

Key Hierarchy

MSK -> PMK-R0

If the negotiated AKM is 00-0F-AC:3, then Q = 256 and

— MPMK = L(MSK, 256, 256), i.e., the second 256 bits of the MSK (which is derived from the IEEE 802.1X authentication)

The PMK-R0 is then derived as follows:

R0-Key-Data = KDF-Hash-Length(XXKey, "FT-R0", SSIDlength || SSID || MDID || R0KHlength || R0KH-ID || S0KH-ID)

PMK-R0 = L(R0-Key-Data, 0, Q)

PMK-R0Name-Salt = L(R0-Key-Data, Q, 128)

Length = Q + 128

IEEE Std 802.11-2020, 12.7.1.6.3 PMK-R0

Key Hierarchy

- **PMK-R0 -> PMK-R1**

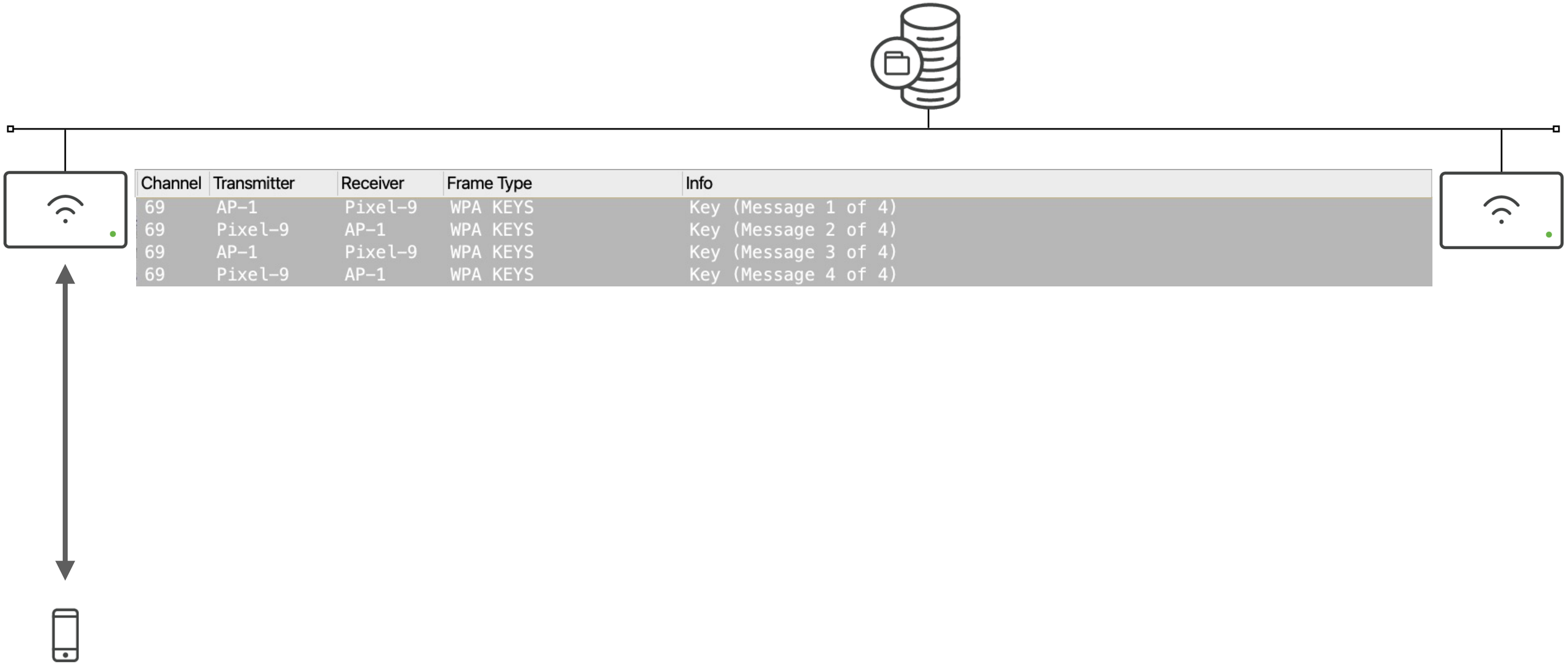
PMK-R1 = KDF-Hash-Length(PMK-R0, “FT-R1”, R1KH-ID || S1KH-ID)

IEEE Std 802.11-2020, 12.7.1.6.4 PMK-R1

The computation of PMK-R0 and PMK-R1, and all of the intermediate results in the computations, shall be restricted to the R0KH.

13.2.1 Introduction

Frame by Frame



Channel	Transmitter	Receiver	Frame Type	Info
69	AP-1	Pixel-9	WPA KEYS	Key (Message 1 of 4)
69	Pixel-9	AP-1	WPA KEYS	Key (Message 2 of 4)
69	AP-1	Pixel-9	WPA KEYS	Key (Message 3 of 4)
69	Pixel-9	AP-1	WPA KEYS	Key (Message 4 of 4)

Key Hierarchy

- **PMK-R1 -> PTK**

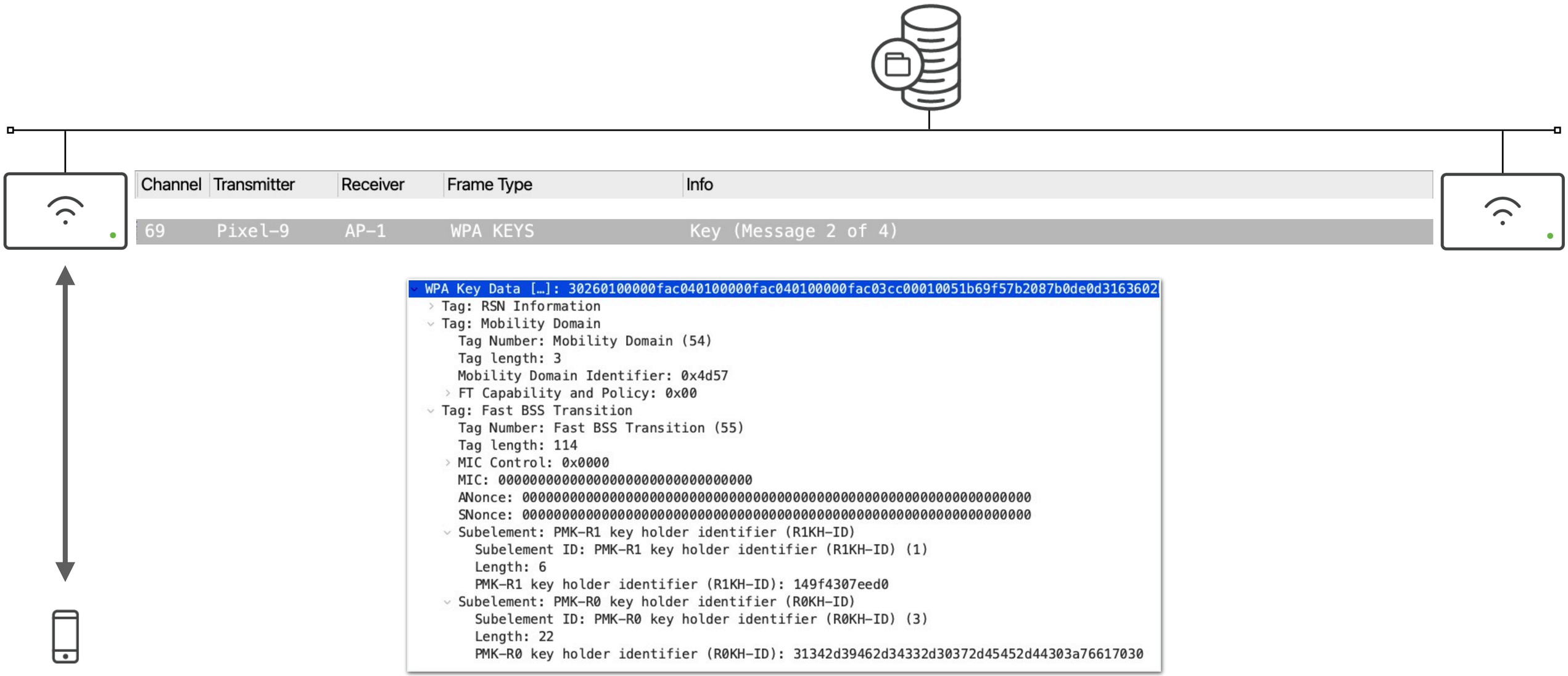
PTK = KDF-Hash-Length(PMK-R1, “FT-PTK”, SNonce || ANonce || BSSID || STA-ADDR)

IEEE Std 802.11-2020, 12.7.1.6.5 PTK

The computation of PTK, and all intermediate results in its computation, shall be restricted to the R1KH.

13.2.1 Introduction

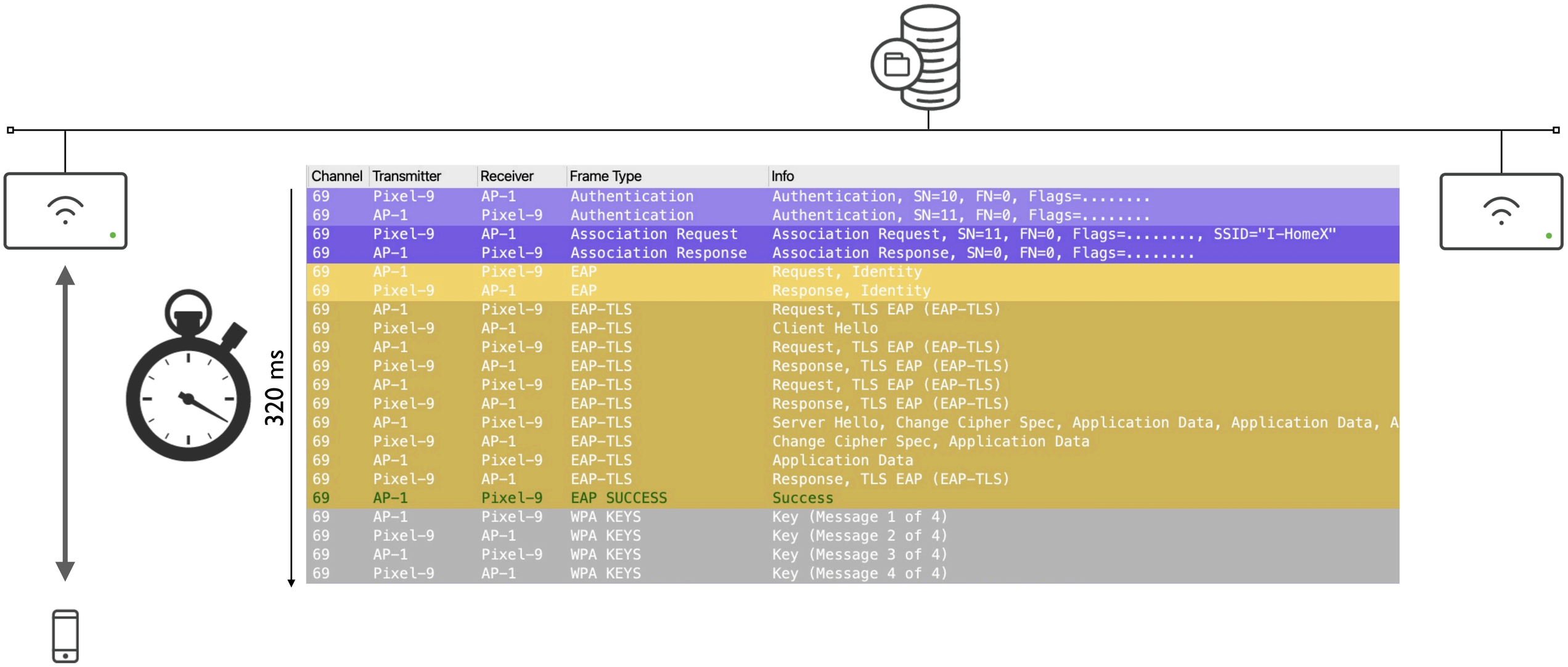
Frame by Frame



Channel	Transmitter	Receiver	Frame Type	Info
69	Pixel-9	AP-1	WPA KEYS	Key (Message 2 of 4)

```
WPA Key Data […]: 30260100000fac040100000fac040100000fac03cc00010051b69f57b2087b0de0d3163602
  Tag: RSN Information
  Tag: Mobility Domain
    Tag Number: Mobility Domain (54)
    Tag length: 3
    Mobility Domain Identifier: 0x4d57
    FT Capability and Policy: 0x00
  Tag: Fast BSS Transition
    Tag Number: Fast BSS Transition (55)
    Tag length: 114
    MIC Control: 0x0000
    MIC: 00000000000000000000000000000000
    ANonce: 0000000000000000000000000000000000000000000000000000000000000000
    SNonce: 0000000000000000000000000000000000000000000000000000000000000000
    Subelement: PMK-R1 key holder identifier (R1KH-ID)
      Subelement ID: PMK-R1 key holder identifier (R1KH-ID) (1)
      Length: 6
      PMK-R1 key holder identifier (R1KH-ID): 149f4307eed0
    Subelement: PMK-R0 key holder identifier (R0KH-ID)
      Subelement ID: PMK-R0 key holder identifier (R0KH-ID) (3)
      Length: 22
      PMK-R0 key holder identifier (R0KH-ID): 31342d39462d34332d30372d45452d44303a76617030
```

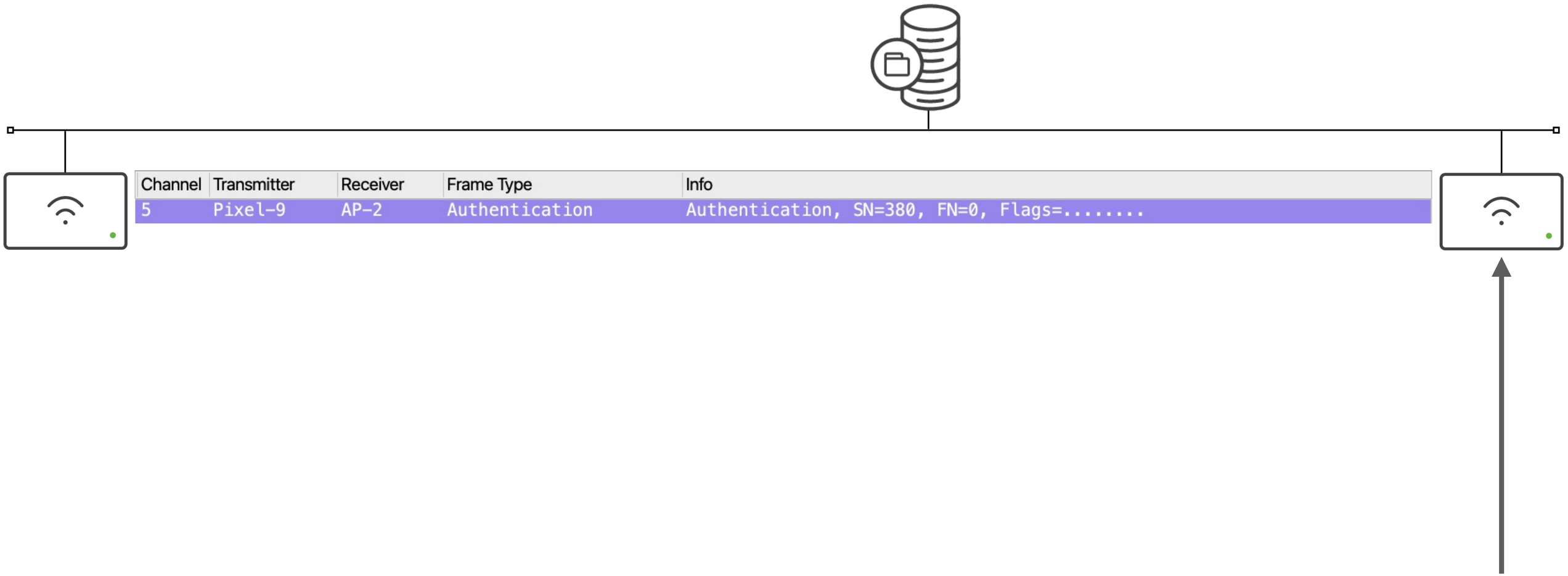
Frame by Frame



Channel	Transmitter	Receiver	Frame Type	Info
69	Pixel-9	AP-1	Authentication	Authentication, SN=10, FN=0, Flags=........
69	AP-1	Pixel-9	Authentication	Authentication, SN=11, FN=0, Flags=........
69	Pixel-9	AP-1	Association Request	Association Request, SN=11, FN=0, Flags=........, SSID="I-HomeX"
69	AP-1	Pixel-9	Association Response	Association Response, SN=0, FN=0, Flags=........
69	AP-1	Pixel-9	EAP	Request, Identity
69	Pixel-9	AP-1	EAP	Response, Identity
69	AP-1	Pixel-9	EAP-TLS	Request, TLS EAP (EAP-TLS)
69	Pixel-9	AP-1	EAP-TLS	Client Hello
69	AP-1	Pixel-9	EAP-TLS	Request, TLS EAP (EAP-TLS)
69	Pixel-9	AP-1	EAP-TLS	Response, TLS EAP (EAP-TLS)
69	AP-1	Pixel-9	EAP-TLS	Request, TLS EAP (EAP-TLS)
69	Pixel-9	AP-1	EAP-TLS	Response, TLS EAP (EAP-TLS)
69	AP-1	Pixel-9	EAP-TLS	Server Hello, Change Cipher Spec, Application Data, Application Data, A
69	Pixel-9	AP-1	EAP-TLS	Change Cipher Spec, Application Data
69	AP-1	Pixel-9	EAP-TLS	Application Data
69	Pixel-9	AP-1	EAP-TLS	Response, TLS EAP (EAP-TLS)
69	AP-1	Pixel-9	EAP SUCCESS	Success
69	AP-1	Pixel-9	WPA KEYS	Key (Message 1 of 4)
69	Pixel-9	AP-1	WPA KEYS	Key (Message 2 of 4)
69	AP-1	Pixel-9	WPA KEYS	Key (Message 3 of 4)
69	Pixel-9	AP-1	WPA KEYS	Key (Message 4 of 4)

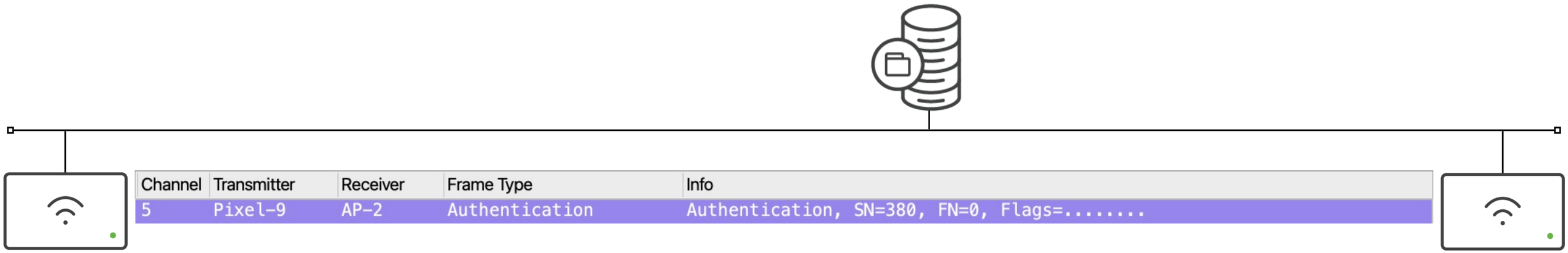
320 ms

Frame by Frame



Channel	Transmitter	Receiver	Frame Type	Info
5	Pixel-9	AP-2	Authentication	Authentication, SN=380, FN=0, Flags=........

Frame by Frame

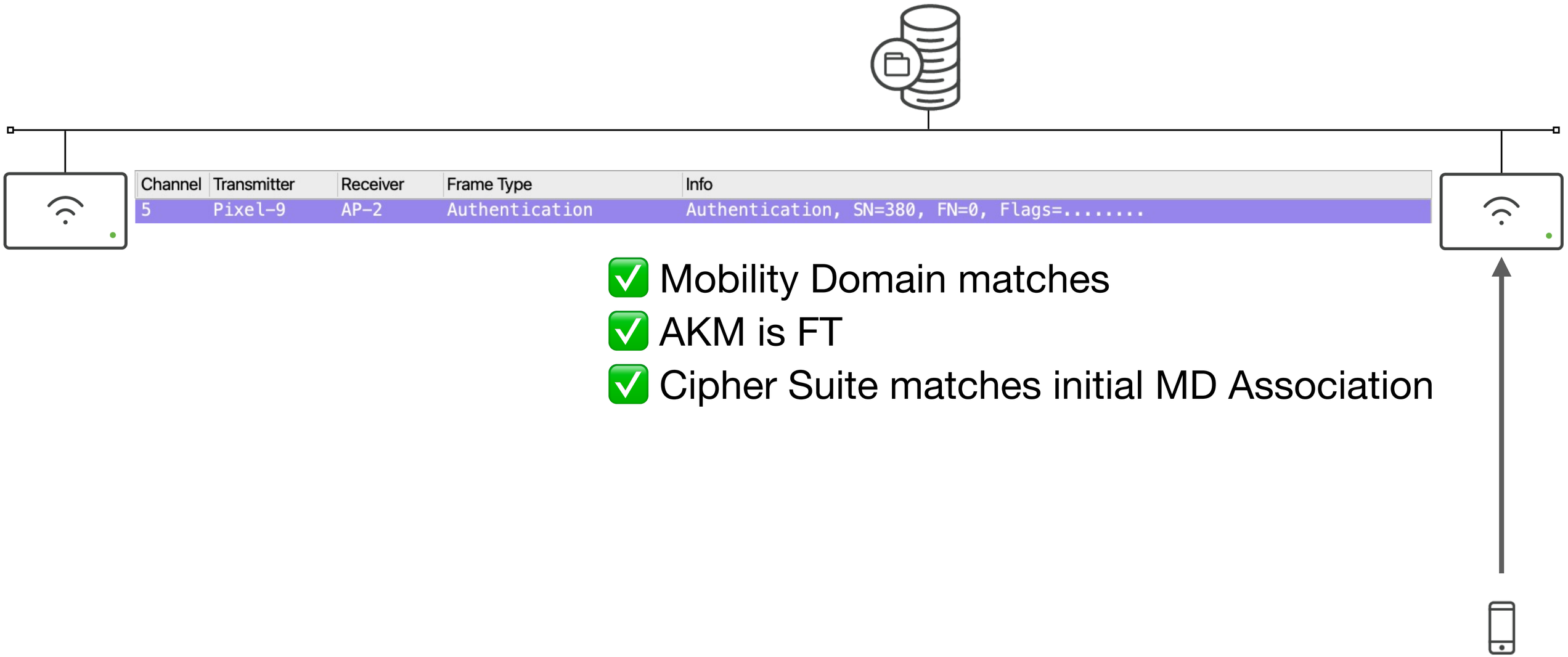


Channel	Transmitter	Receiver	Frame Type	Info
5	Pixel-9	AP-2	Authentication	Authentication, SN=380, FN=0, Flags=........

```
IEEE 802.11 Wireless Management
  Fixed parameters (6 bytes)
    Authentication Algorithm: Fast BSS Transition (2)
    Authentication SEQ: 0x0001
    Status code: Successful (0x0000)
  Tagged parameters (165 bytes)
    Tag: RSN Information
      Tag Number: RSN Information (48)
      Tag length: 38
      RSN Version: 1
    > Group Cipher Suite: 00:0f:ac (Ieee 802.11) AES (CCM)
      Pairwise Cipher Suite Count: 1
    > Pairwise Cipher Suite List 00:0f:ac (Ieee 802.11) AES (CCM)
      Auth Key Management (AKM) Suite Count: 1
    > Auth Key Management (AKM) List 00:0f:ac (Ieee 802.11) FT over IEEE 802.1X
    > RSN Capabilities: 0x00cc
      PMKID Count: 1
    v PMKID List
        PMKID: df0073520ec47f7df2d7f79668efe293
```

```
Tag: Mobility Domain
  Tag Number: Mobility Domain (54)
  Tag length: 3
  Mobility Domain Identifier: 0x4d57
> FT Capability and Policy: 0x00
```

Frame by Frame



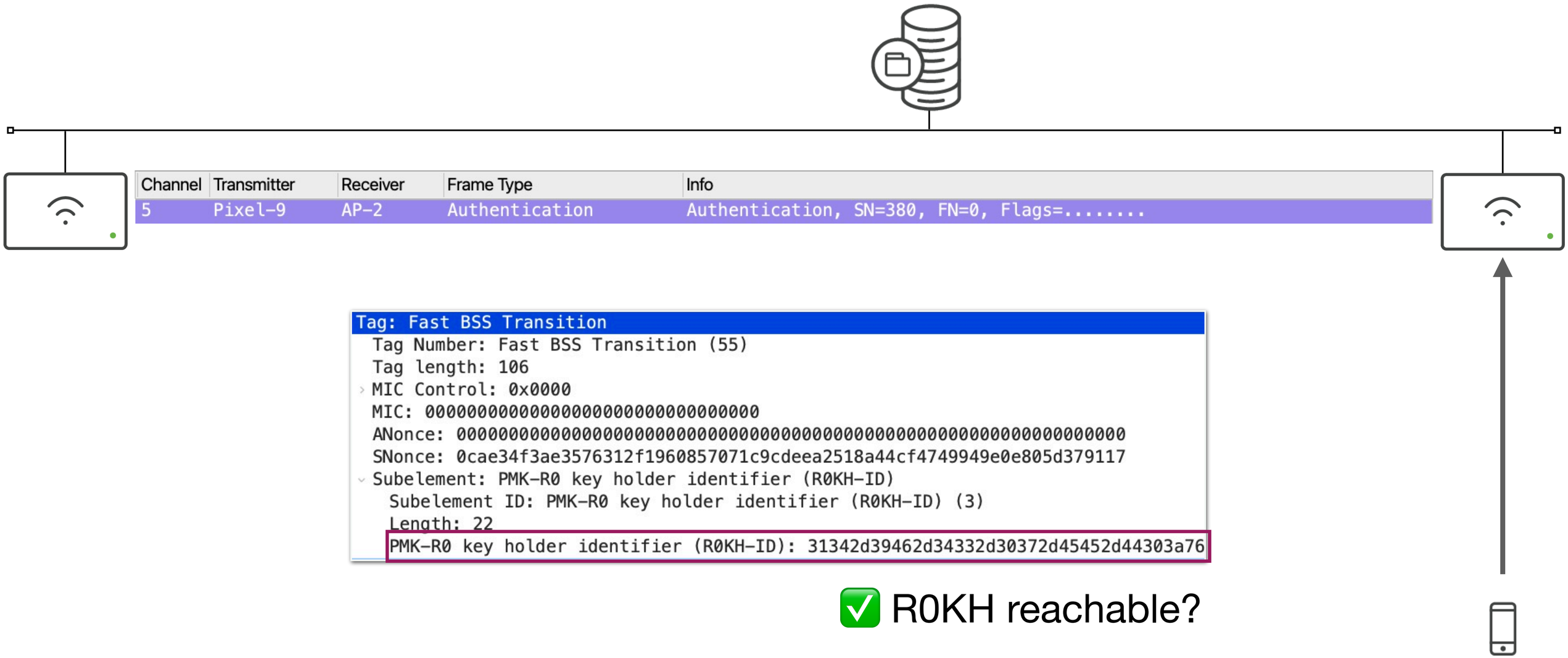
Channel	Transmitter	Receiver	Frame Type	Info
5	Pixel-9	AP-2	Authentication	Authentication, SN=380, FN=0, Flags=........

✅ Mobility Domain matches

✅ AKM is FT

✅ Cipher Suite matches initial MD Association

Frame by Frame

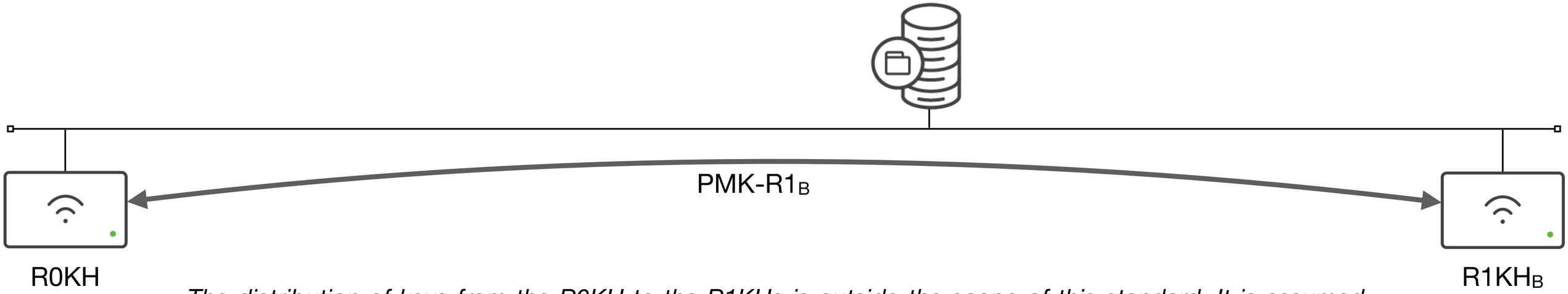


Channel	Transmitter	Receiver	Frame Type	Info
5	Pixel-9	AP-2	Authentication	Authentication, SN=380, FN=0, Flags=........

```
Tag: Fast BSS Transition
  Tag Number: Fast BSS Transition (55)
  Tag length: 106
> MIC Control: 0x0000
  MIC: 00000000000000000000000000000000
  ANonce: 0000000000000000000000000000000000000000000000000000000000000000
  SNonce: 0cae34f3ae3576312f1960857071c9cdeea2518a44cf4749949e0e805d379117
v Subelement: PMK-R0 key holder identifier (R0KH-ID)
    Subelement ID: PMK-R0 key holder identifier (R0KH-ID) (3)
    Length: 22
    PMK-R0 key holder identifier (R0KH-ID): 31342d39462d34332d30372d45452d44303a76
```

✅ R0KH reachable?

Frame by Frame



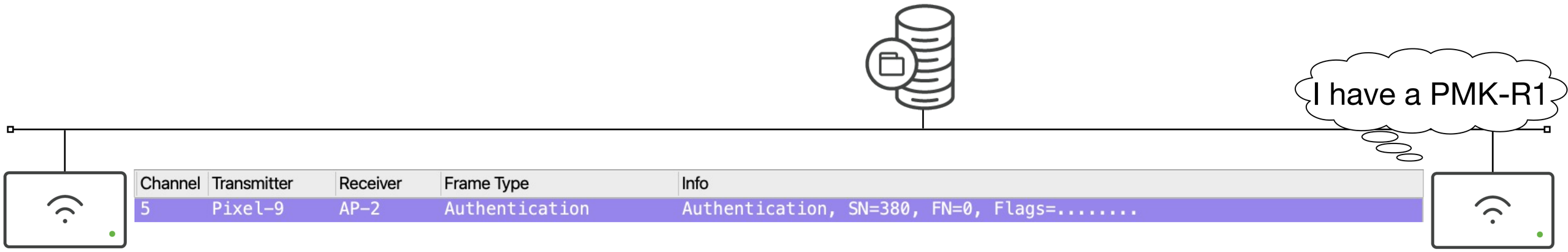
The distribution of keys from the R0KH to the R1KHs is outside the scope of this standard. It is assumed that the PMK-R1s are distributed from the R0KH to the R1KHs following the requirements specified in 13.2.2.

12.7.1.6.1 Overview

The R0KH and the R1KH are assumed to have a secure channel between them that can be used to exchange cryptographic keys without exposure to any intermediate parties. ***The cryptographic strength of the secure channel between the R0KH and R1KH is assumed to be greater than or equal to the cryptographic strength of the channels for which the keys are used****.*

13.2.2 Authenticator key holders

Frame by Frame



Channel	Transmitter	Receiver	Frame Type	Info
5	Pixel-9	AP-2	Authentication	Authentication, SN=380, FN=0, Flags=........

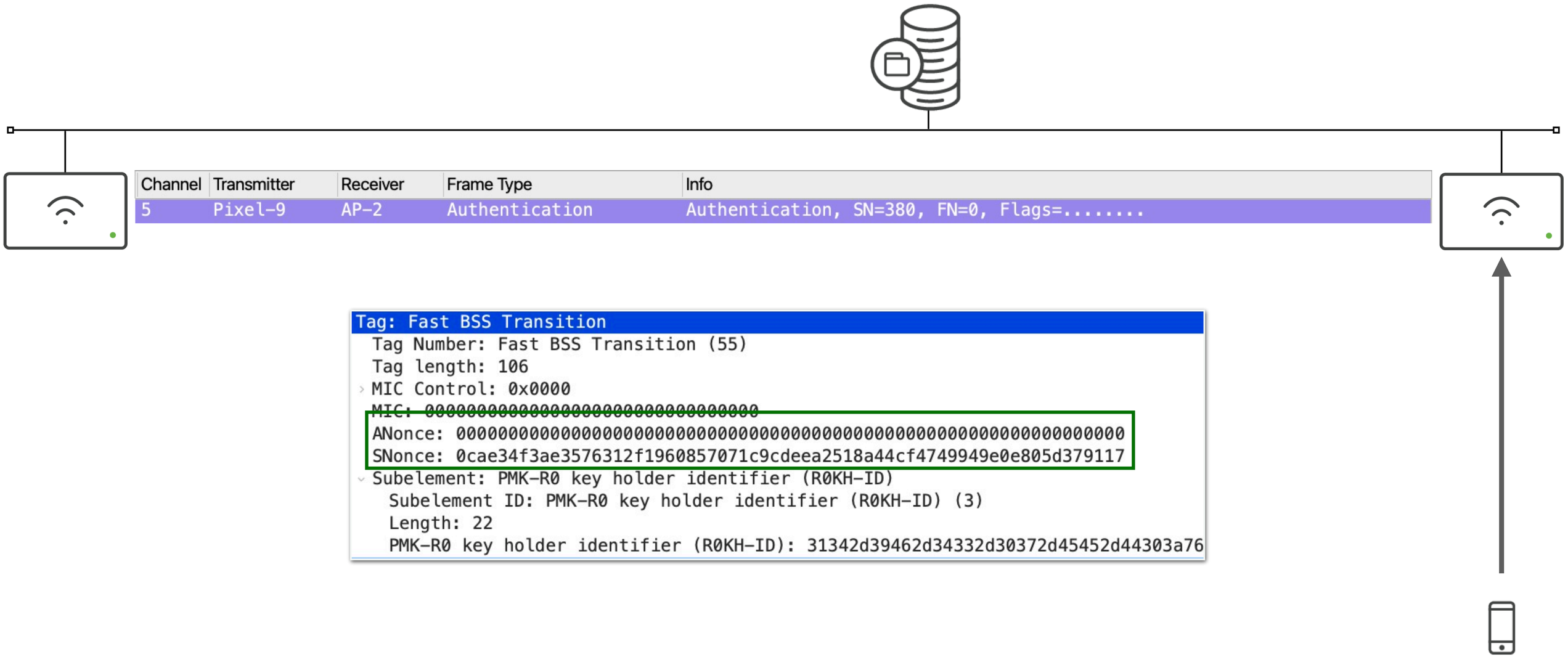
```
IEEE 802.11 Wireless Management
  Fixed parameters (6 bytes)
    Authentication Algorithm: Fast BSS Transition (2)
    Authentication SEQ: 0x0001
    Status code: Successful (0x0000)
  Tagged parameters (165 bytes)
    Tag: RSN Information
      Tag Number: RSN Information (48)
      Tag length: 38
      RSN Version: 1
      Group Cipher Suite: 00:0f:ac (Ieee 802.11) AES (CCM)
      Pairwise Cipher Suite Count: 1
      Pairwise Cipher Suite List 00:0f:ac (Ieee 802.11) AES (CCM)
      Auth Key Management (AKM) Suite Count: 1
      Auth Key Management (AKM) List 00:0f:ac (Ieee 802.11) FT over IEEE 802.1X
      RSN Capabilities: 0x00cc
      PMKID Count: 1
      PMKID List
        PMKID: df0073520ec47f7df2d7f79668efe293
```

PMKR0Name

↓

PMKR1Name

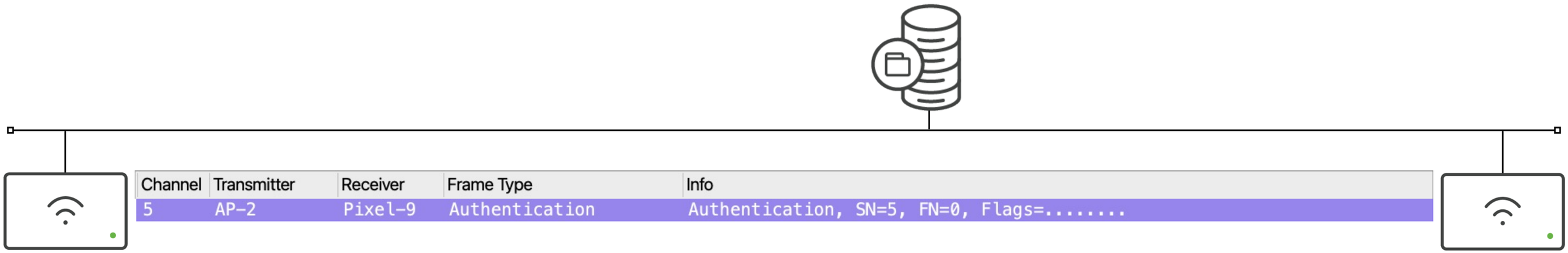
Frame by Frame



Channel	Transmitter	Receiver	Frame Type	Info
5	Pixel-9	AP-2	Authentication	Authentication, SN=380, FN=0, Flags=........

```
Tag: Fast BSS Transition
  Tag Number: Fast BSS Transition (55)
  Tag length: 106
> MIC Control: 0x0000
  MIC: 00000000000000000000000000000000
  ANonce: 0000000000000000000000000000000000000000000000000000000000000000
  SNonce: 0cae34f3ae3576312f1960857071c9cdeea2518a44cf4749949e0e805d379117
v Subelement: PMK-R0 key holder identifier (R0KH-ID)
    Subelement ID: PMK-R0 key holder identifier (R0KH-ID) (3)
    Length: 22
    PMK-R0 key holder identifier (R0KH-ID): 31342d39462d34332d30372d45452d44303a76
```

Frame by Frame

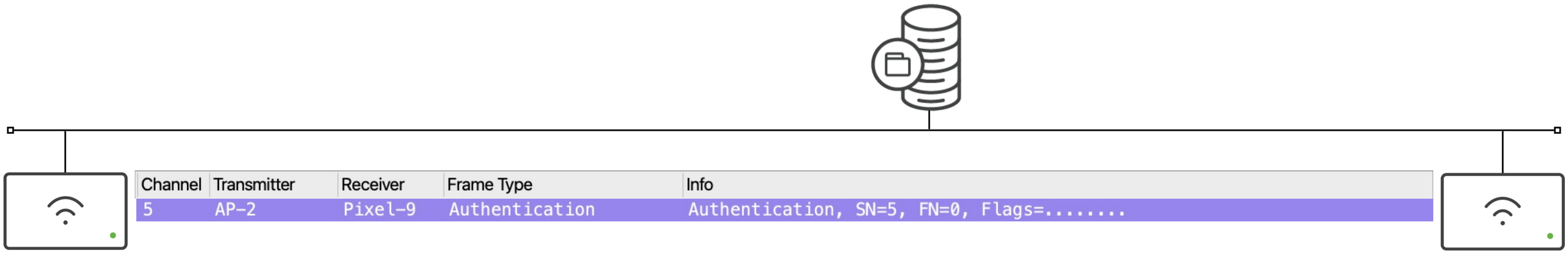


Channel	Transmitter	Receiver	Frame Type	Info
5	AP-2	Pixel-9	Authentication	Authentication, SN=5, FN=0, Flags=........

```
IEEE 802.11 Wireless Management
▾ Fixed parameters (6 bytes)
    Authentication Algorithm: Fast BSS Transition (2)
    Authentication SEQ: 0x0002
    Status code: Successful (0x0000)
▾ Tagged parameters (165 bytes)
  ▾ Tag: RSN Information
      Tag Number: RSN Information (48)
      Tag length: 42
      RSN Version: 1
    › Group Cipher Suite: 00:0f:ac (Ieee 802.11) AES (CCM)
      Pairwise Cipher Suite Count: 1
    › Pairwise Cipher Suite List 00:0f:ac (Ieee 802.11) AES (CCM)
      Auth Key Management (AKM) Suite Count: 2
    ▾ Auth Key Management (AKM) List 00:0f:ac (Ieee 802.11) FT over IEEE 802.1X 00:0f:a
      › Auth Key Management (AKM) Suite: 00:0f:ac (Ieee 802.11) FT over IEEE 802.1X
      › Auth Key Management (AKM) Suite: 00:0f:ac (Ieee 802.11) WPA (SHA256)
    › RSN Capabilities: 0x00c0
      PMKID Count: 1
    ▾ PMKID List
        PMKID: df0073520ec47f7df2d7f79668efe293
```

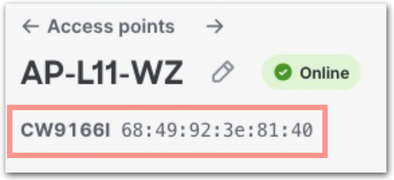
```
Tag: Mobility Domain
  Tag Number: Mobility Domain (54)
  Tag length: 3
  Mobility Domain Identifier: 0x4d57
› FT Capability and Policy: 0x00
```

Frame by Frame

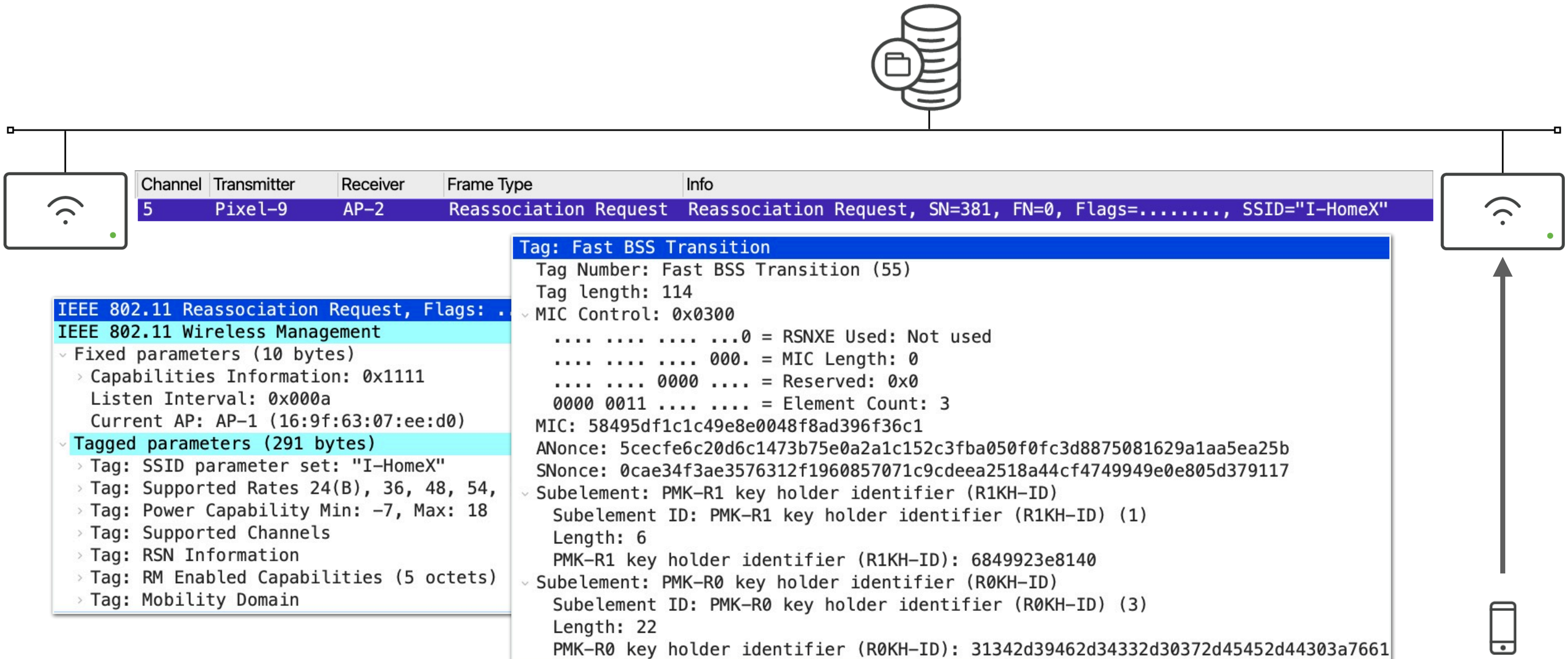


Channel	Transmitter	Receiver	Frame Type	Info
5	AP-2	Pixel-9	Authentication	Authentication, SN=5, FN=0, Flags=........

```
Tag: Fast BSS Transition
  Tag Number: Fast BSS Transition (55)
  Tag length: 114
› MIC Control: 0x0000
  MIC: 00000000000000000000000000000000
  ANonce: 5cecfe6c20d6c1473b75e0a2a1c152c3fba050f0fc3d8875081629a1aa5ea25b
  SNonce: 0cae34f3ae3576312f1960857071c9cdeea2518a44cf4749949e0e805d379117
⌄ Subelement: PMK-R1 key holder identifier (R1KH-ID)
    Subelement ID: PMK-R1 key holder identifier (R1KH-ID) (1)
    Length: 6
    PMK-R1 key holder identifier (R1KH-ID): 6849923e8140
⌄ Subelement: PMK-R0 key holder identifier (R0KH-ID)
    Subelement ID: PMK-R0 key holder identifier (R0KH-ID) (3)
    Length: 22
    PMK-R0 key holder identifier (R0KH-ID): 31342d39462d34332d30372d45452d44303a7661
```



Frame by Frame

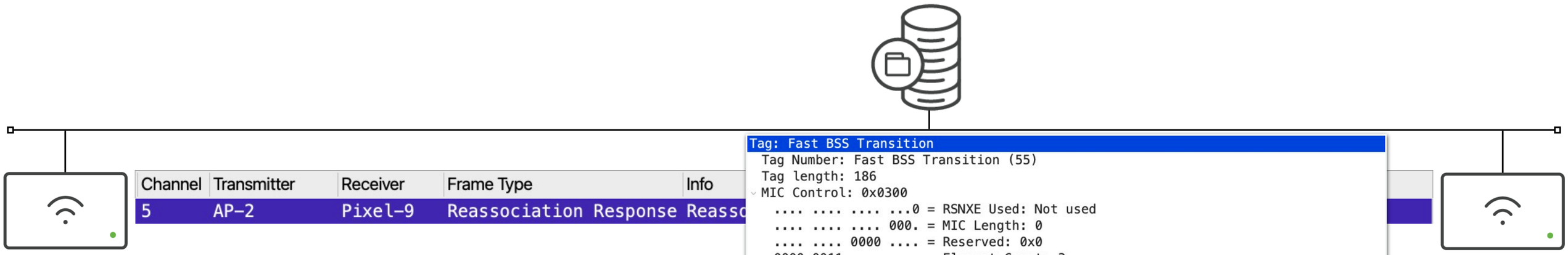


Channel	Transmitter	Receiver	Frame Type	Info
5	Pixel-9	AP-2	Reassociation Request	Reassociation Request, SN=381, FN=0, Flags=........, SSID="I-HomeX"

```
IEEE 802.11 Reassociation Request, Flags: ..
IEEE 802.11 Wireless Management
  Fixed parameters (10 bytes)
    Capabilities Information: 0x1111
    Listen Interval: 0x000a
    Current AP: AP-1 (16:9f:63:07:ee:d0)
  Tagged parameters (291 bytes)
    Tag: SSID parameter set: "I-HomeX"
    Tag: Supported Rates 24(B), 36, 48, 54,
    Tag: Power Capability Min: -7, Max: 18
    Tag: Supported Channels
    Tag: RSN Information
    Tag: RM Enabled Capabilities (5 octets)
    Tag: Mobility Domain
```

```
Tag: Fast BSS Transition
  Tag Number: Fast BSS Transition (55)
  Tag length: 114
  MIC Control: 0x0300
    .... .... .... ...0 = RSNXE Used: Not used
    .... .... .... 000. = MIC Length: 0
    .... .... 0000 .... = Reserved: 0x0
    0000 0011 .... .... = Element Count: 3
  MIC: 58495df1c1c49e8e0048f8ad396f36c1
  ANonce: 5cecfe6c20d6c1473b75e0a2a1c152c3fba050f0fc3d8875081629a1aa5ea25b
  SNonce: 0cae34f3ae3576312f1960857071c9cdeea2518a44cf4749949e0e805d379117
  Subelement: PMK-R1 key holder identifier (R1KH-ID)
    Subelement ID: PMK-R1 key holder identifier (R1KH-ID) (1)
    Length: 6
    PMK-R1 key holder identifier (R1KH-ID): 6849923e8140
  Subelement: PMK-R0 key holder identifier (R0KH-ID)
    Subelement ID: PMK-R0 key holder identifier (R0KH-ID) (3)
    Length: 22
    PMK-R0 key holder identifier (R0KH-ID): 31342d39462d34332d30372d45452d44303a7661
```

Frame by Frame



Channel	Transmitter	Receiver	Frame Type	Info
5	AP-2	Pixel-9	Reassociation Response	Reassc

```
IEEE 802.11 Reassociation Response, Flags: ........
IEEE 802.11 Wireless Management
  Fixed parameters (6 bytes)
    Capabilities Information: 0x1511
    Status code: Successful (0x0000)
    ..00 0000 0000 0101 = Association ID: 0x0005
  Tagged parameters (400 bytes)
    Tag: Supported Rates 24(B), 36, 48, 54, [Mbit/sec]
    Tag: RM Enabled Capabilities (5 octets)
    Tag: RSN Information
    Tag: Mobility Domain
```

```
Tag: Fast BSS Transition
  Tag Number: Fast BSS Transition (55)
  Tag length: 186
  MIC Control: 0x0300
    .... .... .... ...0 = RSNXE Used: Not used
    .... .... .... 000. = MIC Length: 0
    .... .... 0000 .... = Reserved: 0x0
    0000 0011 .... .... = Element Count: 3
  MIC: 6fe97f0065228409c2904c48e4bbdda4
  ANonce: 5cecfe6c20d6c1473b75e0a2a1c152c3fba050f0fc3d8875081629a1aa5ea25b
  SNonce: 0cae34f3ae3576312f1960857071c9cdeea2518a44cf4749949e0e805d379117
  Subelement: PMK-R1 key holder identifier (R1KH-ID)
    Subelement ID: PMK-R1 key holder identifier (R1KH-ID) (1)
    Length: 6
    PMK-R1 key holder identifier (R1KH-ID): 6849923e8140
  Subelement: PMK-R0 key holder identifier (R0KH-ID)
    Subelement ID: PMK-R0 key holder identifier (R0KH-ID) (3)
    Length: 22
    PMK-R0 key holder identifier (R0KH-ID): 31342d39462d34332d30372d45452d44303a7661
  Subelement: GTK subelement
    Subelement ID: GTK subelement (2)
    Length: 35
    Key Info: 0x0002
    .... .... .... ..10 = Key ID: 2
    Key Length: 16
    RSC: c008000000000000
    GTK (encrypted): 46592a2accf842eb8119bc941a44f2e2b943be851ed69e8d
  Subelement: IGTK
    Subelement ID: IGTK (4)
    Length: 33
    Key ID: 5
    IPN: 000000000000
    Key Length: 16
    Wrapped Key (IGTK): a1d9a4fdc7aa2223bcab99134509fdbc9860d9cb4872579e
```

Frame by Frame

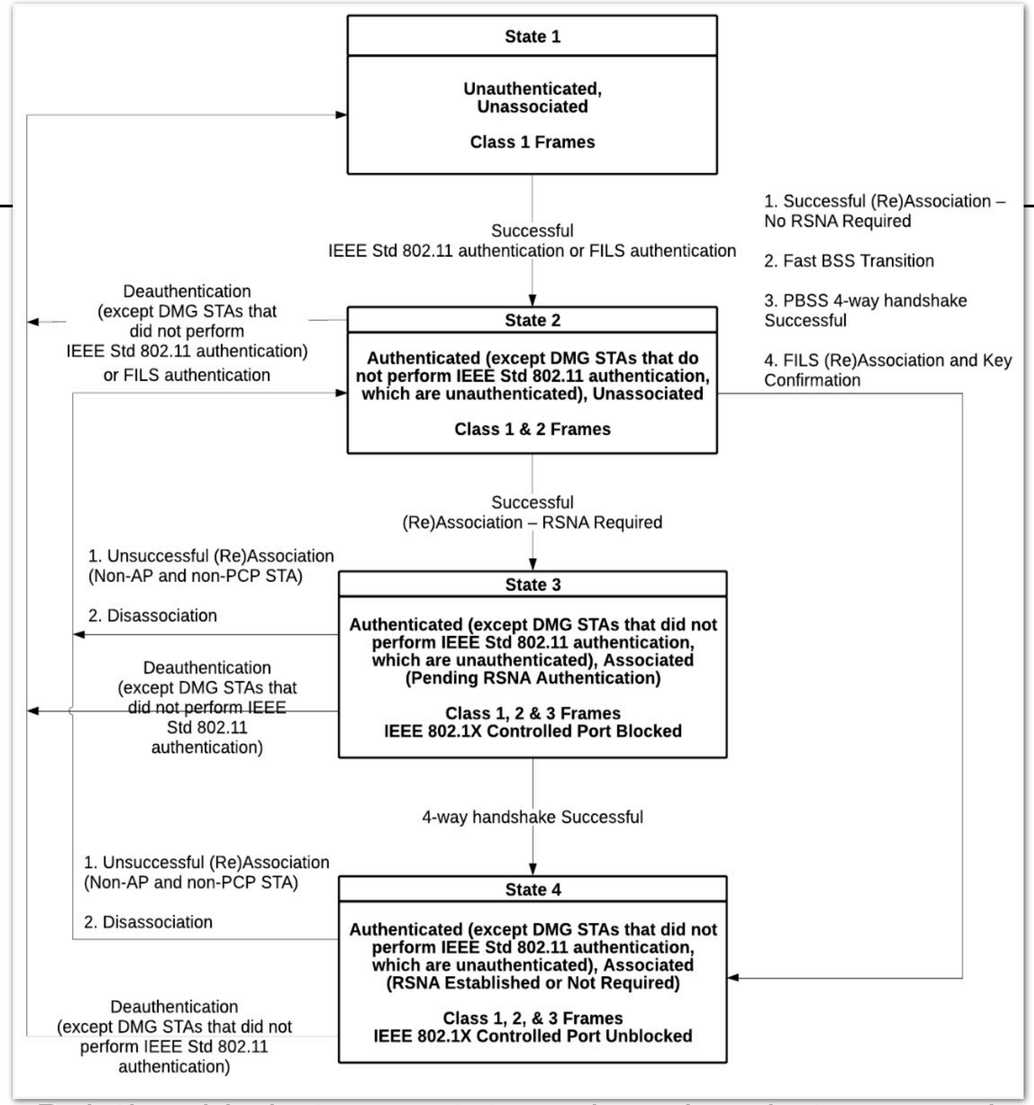


Figure 11-17—Relationship between state and services between a given pair of nonmesh STAs

The SME of the AP shall open the IEEE 802.1X Controlled Port.

The FTO shall transition to State 4 (as defined in 11.3).

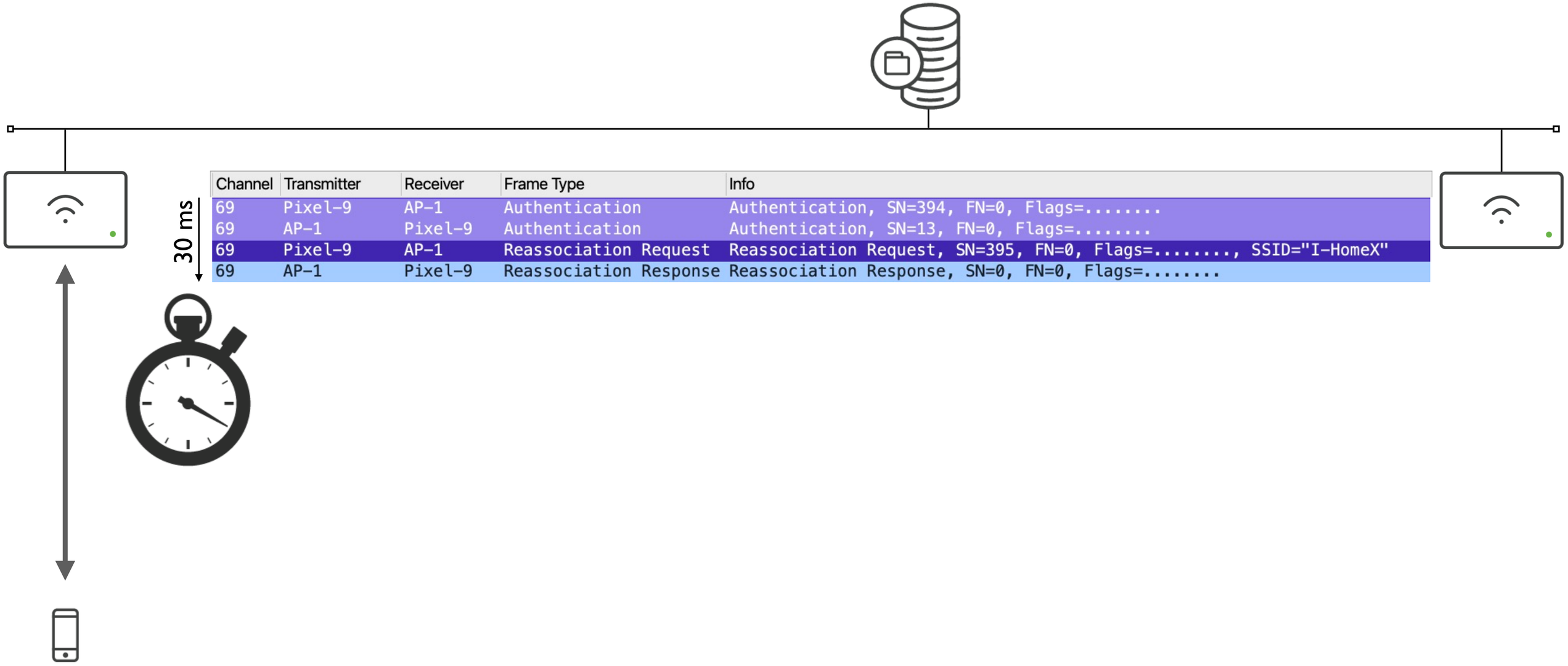
If the target AP is distinct from the previous AP, the FTO shall enter State 1 with respect to the previous AP.

13.7.1 FT reassociation in an RSN

Frame by Frame

Channel	Transmitter	Receiver	Frame Type	Info
5	Pixel-9	AP-2	Authentication	Authentication, SN=380, FN=0, Flags=........
5	AP-2	Pixel-9	Authentication	Authentication, SN=5, FN=0, Flags=........
5	Pixel-9	AP-2	Reassociation Request	Reassociation Request, SN=381, FN=0, Flags=........, SSID="I-HomeX"
5	AP-2	Pixel-9	Reassociation Response	Reassociation Response, SN=0, FN=0, Flags=........

Frame by Frame



Channel	Transmitter	Receiver	Frame Type	Info
69	Pixel-9	AP-1	Authentication	Authentication, SN=394, FN=0, Flags=........
69	AP-1	Pixel-9	Authentication	Authentication, SN=13, FN=0, Flags=........
69	Pixel-9	AP-1	Reassociation Request	Reassociation Request, SN=395, FN=0, Flags=........, SSID="I-HomeX"
69	AP-1	Pixel-9	Reassociation Response	Reassociation Response, SN=0, FN=0, Flags=........

Call to Action

Enable Fast BSS Transition now!

Still not fast enough?

IEEE 802.11bs Standard 2042

Super High Increased Throughput (SHIT) PHY

Data rates up to 42,000 Terabytes