



Getting There with Wireless Mobility & Roaming

Keith Bogart

Cisco CCIE #4923

Key Concepts

- + Roaming Fundamentals & Categories
- + Mobility Groups & Tunneling
- + Layer-3 Inter-Controller Roaming
- + Optimizing Roaming Performance

MAJOR TOPICS

-
- + Roaming Fundamentals
 - + Categories & Types of Roaming
 - + Utilizing Mobility Groups & Tunnels
 - + Layer-3 Inter-Controller Roaming
 - + Reducing Roaming Latency with AP Pre-Selection
 - + Reducing Authentication-Induced Roaming Latency



LEARNING OUTCOMES

- + Explain wireless roaming concepts
- + Describe mobility groups and mobility tunnels
- + Identify roaming triggers and latency factors
- + Configure and verify fast secure roaming techniques
- + Monitor and troubleshoot roaming events
- + Summarize the roaming workflow

-
- + Familiarity with basic 802.11 WLAN terminology
 - + Experience with WPA2 & WPA3
 - + Experience with Cisco Catalyst 9800 Web-UI & Configuration
 - + High-level understanding of 802.1x

PREREQUISITES



LET'S GO!

<https://t.me/learningnets>





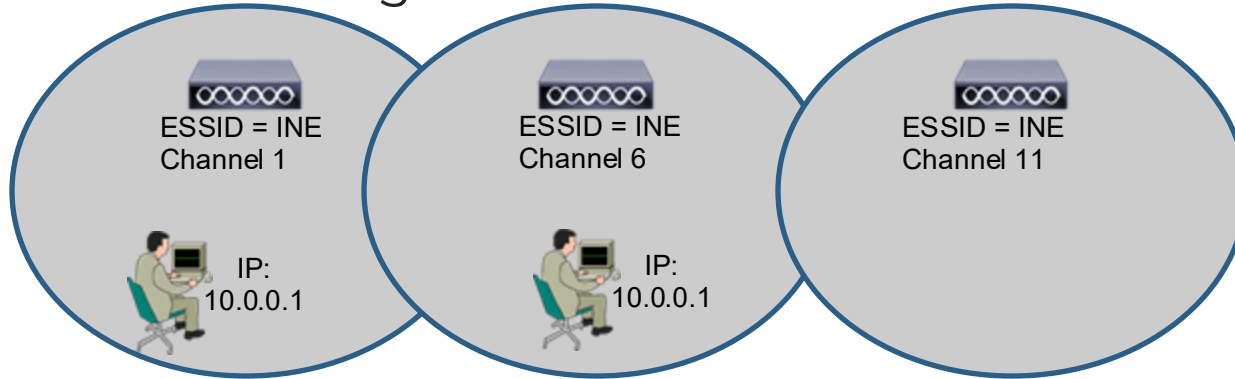
What is Roaming?

What is Wireless Roaming?

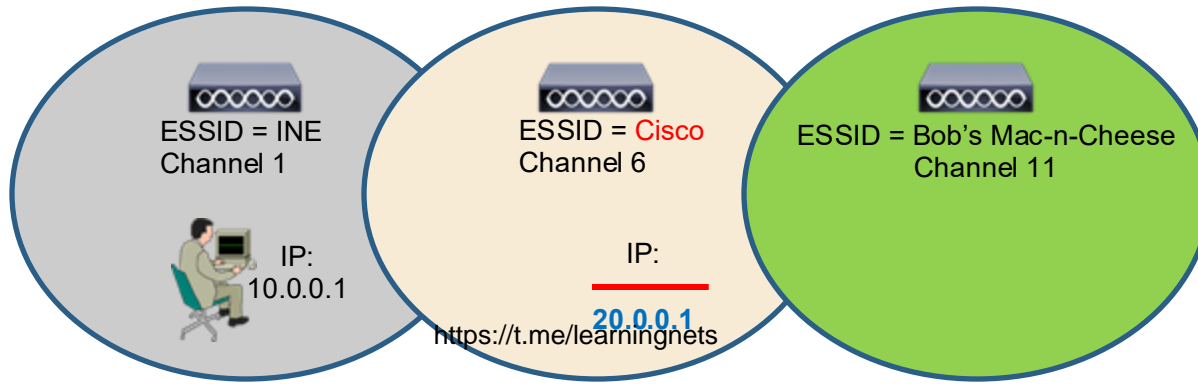
- + Roaming is the process where a wireless client device transitions its connection from one AP to another **without losing network connectivity**.
- + Wireless client must maintain its IPv4/IPv6 address in order to qualify as a roaming event.

Roaming Defined

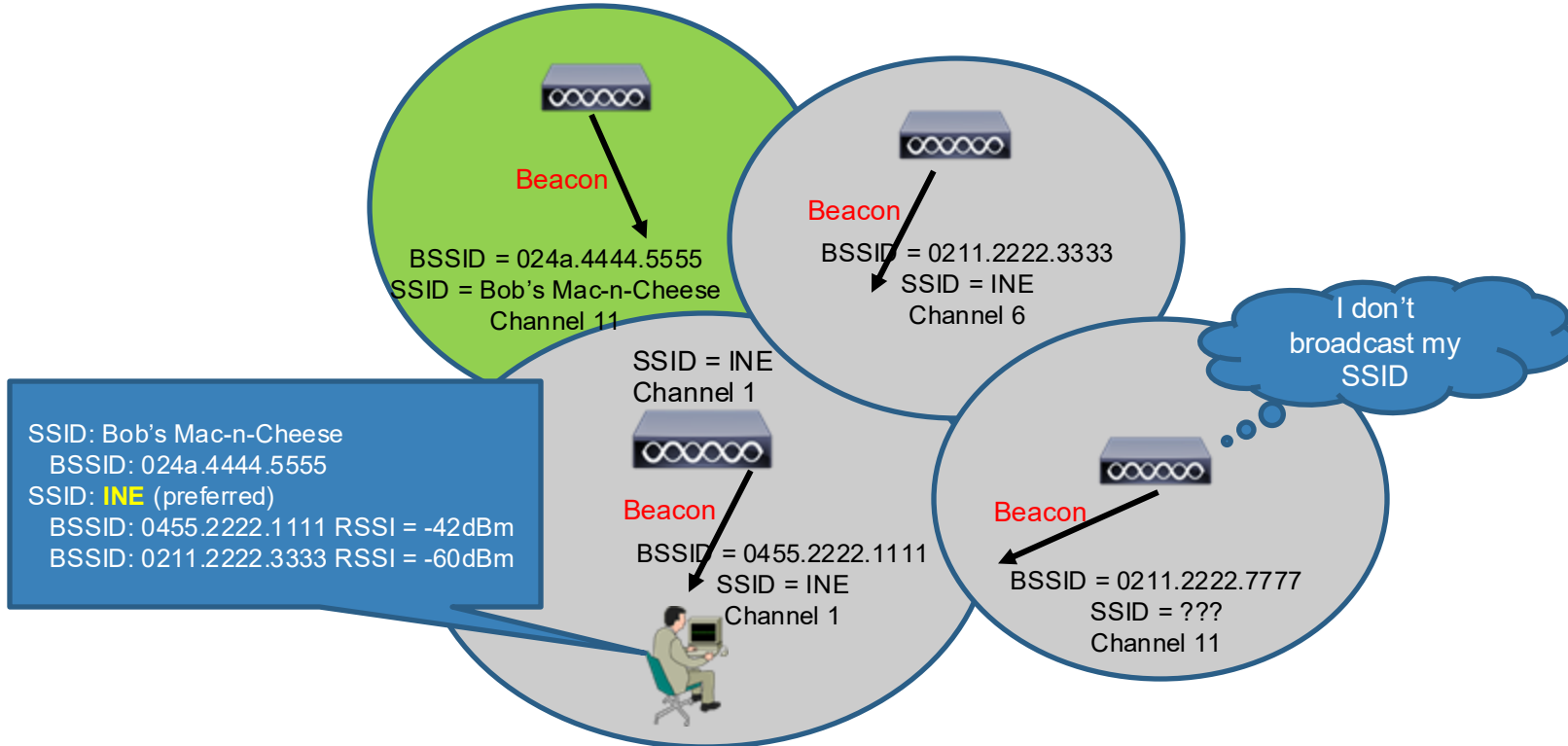
+ What roaming IS



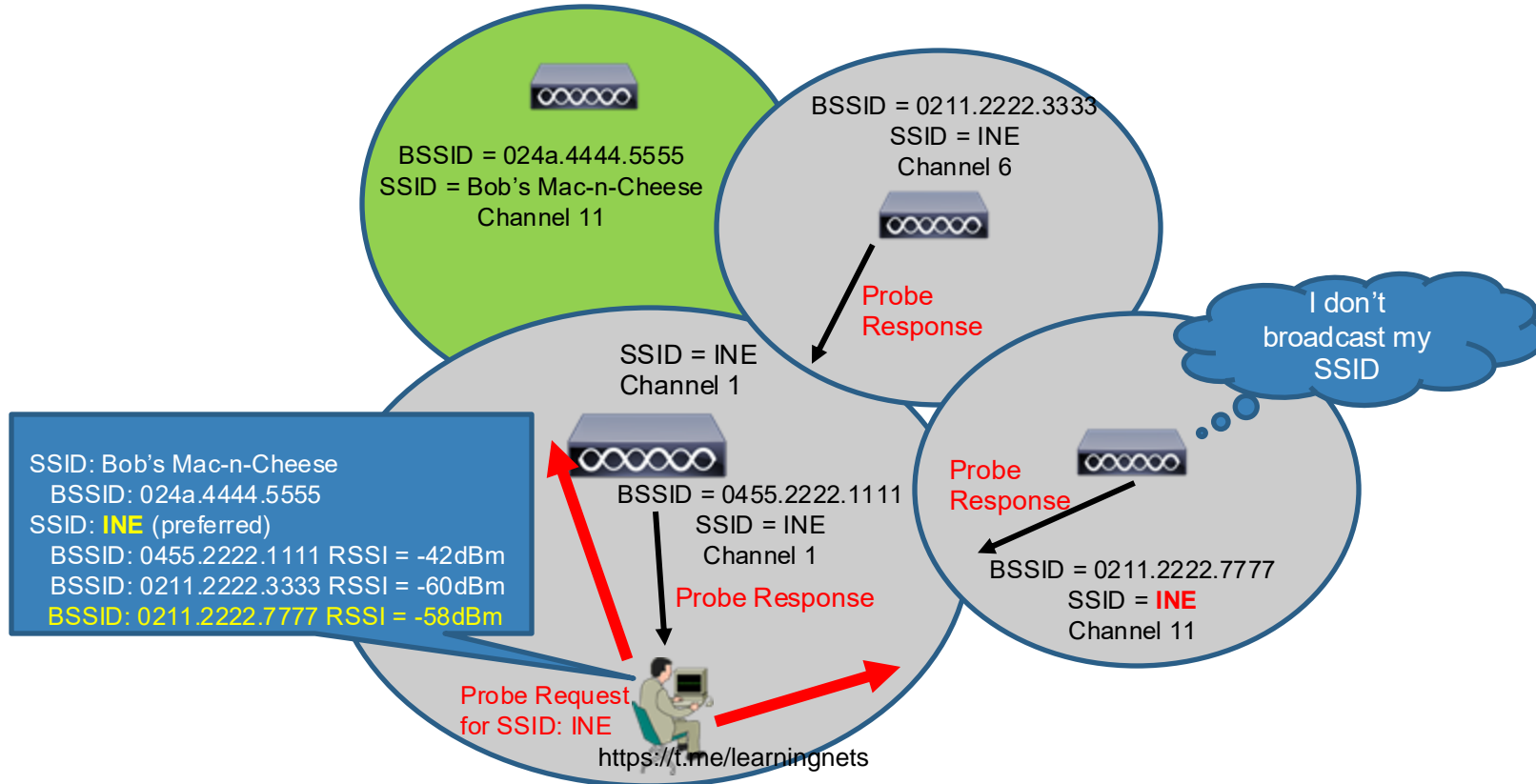
+ What roaming ISN'T



Service Set Learning



Service Set Learning



Roaming Guidelines & Definitions

- + Roaming is defined by two things:
 - + Wi-Fi client makes decision to disassociate from one BSS and associate to another, adjacent BSS
 - + Both former and new BSS **utilize the same SSID**
- + Wi-Fi clients decide when to roam
 - + Clients are always scanning for nearby access points advertising the preferred SSID
 - + RSSI of received Beacons and Probe Responses are evaluated
 - + When RSSI drops below a pre-determined amount (*typically less than -70 to -75dBm*) client will initiate a roam

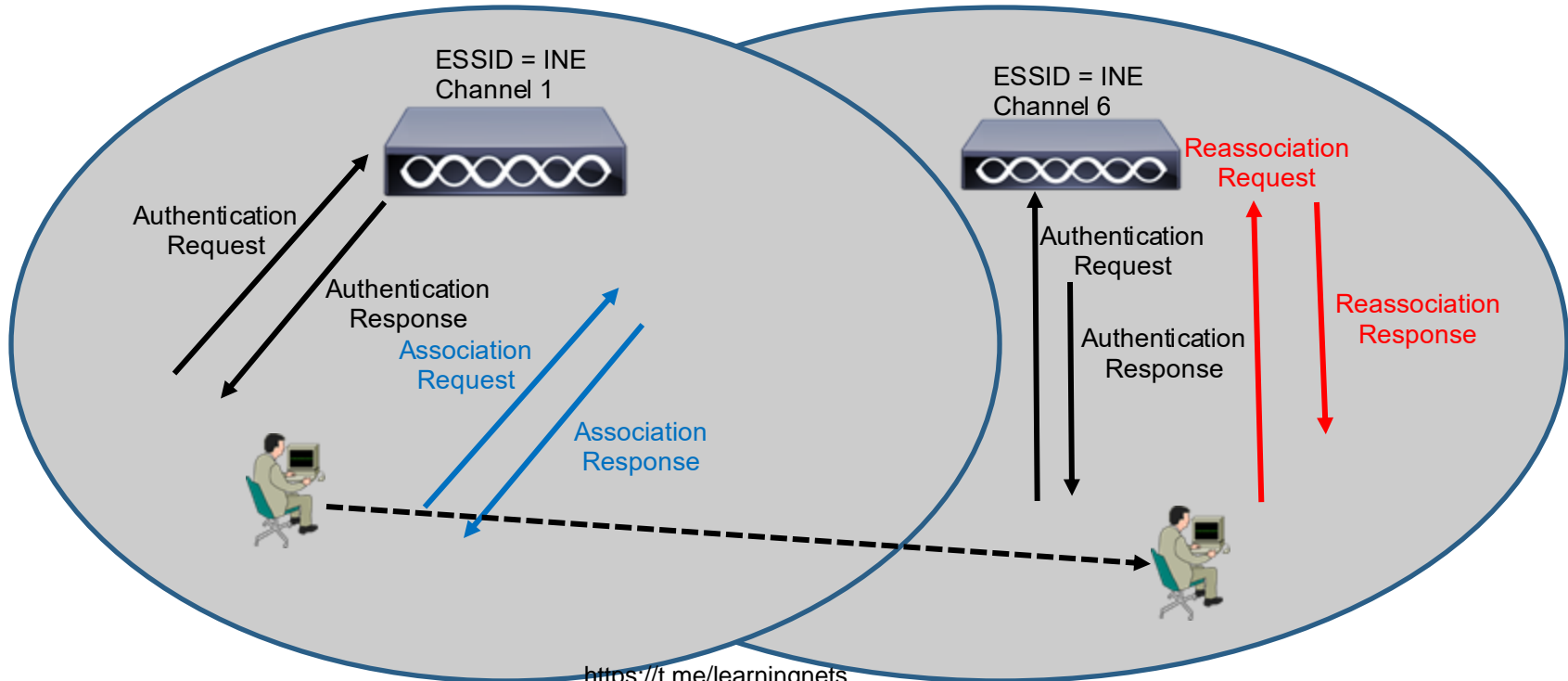
Client Proprietary Algorithms

- + Wi-Fi clients all roam differently
 - + Wi-Fi NIC vendors utilize (secret) proprietary algorithms for roaming decisions
 - + Different Wi-Fi NICs support different roaming optimizations
- + There is no way to know exactly when a client decides to roam.

Roaming aggressiveness settings are not based only on decibel-milliwatts (dBm), but rather on received signal quality (RSSI). This is measured through an algorithm which takes into account several factors such as receive and transmit rates, signal degradation, packet loss percentages, etc, to result in an indexed value. The higher the RSSI value is, the better the signal is.

"Received Signal Strength Indicator," or RSSI, is a measurement of how well your device can hear the signal from your router or access point. dBm and RSSI are different units of measurement that both represent the same thing: signal strength. The difference is that RSSI is a relative index, while dBm is an absolute number representing power levels in mW (milliwatts). RSSI is a term used to measure the relative quality of a received signal to a client device, but has no absolute value (it can be a 0 to 255 value, or vary depending on adapter implementation).

Association & Reassociation



4-Way Handshake

- + Virtually all Wi-Fi networks utilize some form of authentication and encryption
- + Methods used for this purpose originally defined in IEEE 802.11i (now rolled into 802.11-2020 standard)
- + WPA standards include two forms of Wi-Fi authentication:
 - + WPA Personal (uses PSK or SAE)
 - + WPA Enterprise (utilizes 802.1x)
- + Regardless of type used, *a 4-way handshake always ensues after Association or Reassociation*

WPA PSK Handshake

304	2.091412	86:6c:b8:16:5e:89	TpLinkTechno_81:3...	802.11	157	Probe Request, SN=2075, FN=0, Flags=.....C, SSID="SkippyPip"
306	2.092083	TpLinkTechno_81:32:...	86:6c:b8:16:5e:89	802.11	468	Probe Response, SN=2990, FN=0, Flags=.....C, BI=100, SSID="SkippyPip"
308	2.092153	86:6c:b8:16:5e:89	TpLinkTechno_81:3...	802.11	70	Authentication, SN=2076, FN=0, Flags=.....C
310	2.093285	TpLinkTechno_81:32:...	86:6c:b8:16:5e:89	802.11	70	Authentication, SN=2991, FN=0, Flags=.....C
314	2.105668	86:6c:b8:16:5e:89	TpLinkTechno_81:3...	802.11	272	Association Request, SN=2077, FN=0, Flags=.....C, SSID="SkippyPip"
316	2.107910	TpLinkTechno_81:32:...	86:6c:b8:16:5e:89	802.11	248	Association Response, SN=2992, FN=0, Flags=.....C
320	2.119001	TpLinkTechno_81:32:...	86:6c:b8:16:5e:89	EAPOL	171	Key (Message 1 of 4)
330	2.136995	86:6c:b8:16:5e:89	TpLinkTechno_81:3...	EAPOL	193	Key (Message 2 of 4)
332	2.147976	TpLinkTechno_81:32:...	86:6c:b8:16:5e:89	EAPOL	275	Key (Message 3 of 4)
334	2.149832	86:6c:b8:16:5e:89	TpLinkTechno_81:3...	EAPOL	171	Key (Message 4 of 4)

```
> Tag: RM Enabled Capabilities (5 octets)
> Tag: HT Capabilities (802.11n D1.10)
> Tag: HT Information (802.11n D1.10)
> Tag: Overlapping BSS Scan Parameters
> Tag: Extended Capabilities (8 octets)
> Tag: VHT Capabilities
> Tag: VHT Operation
> Tag: Tx Power Envelope
> Tag: Vendor Specific: Microsoft Corp.: WMM/WME: Parameter Element
> Tag: Vendor Specific: Atheros Communications, Inc.: Advanced Capability
> Tag: Vendor Specific: Qualcomm Inc.
> Tag: Vendor Specific: Microsoft Corp.: WPA Information Element
< Tag: RSN Information
  Tag Number: RSN Information (48)
  Tag length: 24
  RSN Version: 1
  > Group Cipher Suite: 00:0f:ac (Ieee 802.11) TKIP
    Pairwise Cipher Suite Count: 2
  > Pairwise Cipher Suite List 00:0f:ac (Ieee 802.11) AES (CCM) 00:0f:ac (Ieee 802.11) TKIP
    Auth Key Management (AKM) Suite Count: 1
  < Auth Key Management (AKM) List 00:0f:ac (Ieee 802.11) PSK
    < Auth Key Management (AKM) Suite: 00:0f:ac (Ieee 802.11) PSK
      Auth Key Management (AKM) OUI: 00:0f:ac (Ieee 802.11)
      Auth Key Management (AKM) type: PSK (2)
```

```
0010 12 0c 99 16 40 01 e7 a5 00 02 00 10 18 03 04 00
0020 02 00 00 00 50 00 3c 00 86 6c b8 16 5e 89 50 d4
0030 f7 81 32 d8 50 d4 f7 81 32 d8 e0 ba 51 e4 10 64
0040 2b 02 00 00 64 00 11 15 00 09 53 6b 69 70 70 79
0050 50 69 70 01 08 8c 12 98 24 b0 48 60 6c 03 01 9d
0060 46 05 73 d0 00 00 0c 2d 1a ef 09 03 ff ff ff 00
0070 00 00 00 00 00 00 00 00 01 00 00 00 00 00 00
0080 00 00 00 3d 16 9d 05 04 00 00 00 00 00 00 00
0090 00 00 00 00 00 00 00 00 00 00 00 4a 0e 14 00 0a
00a0 00 2c 01 c8 00 14 00 05 00 19 00 7f 08 05 00 0f
00b0 02 00 00 00 40 bf 0c f2 79 82 33 ea ff 00 00 ea
00c0 ff 00 20 c0 05 01 9b 00 fc ff c3 05 03 3c 3c 3c
00d0 3c dd 18 00 50 f2 02 01 01 80 00 03 a4 00 00 27
00e0 a4 00 00 42 43 5e 00 62 32 2f 00 dd 09 00 43 7f
00f0 01 01 00 00 ff 7f dd 16 8c fd f0 04 00 00 49 4c
0100 51 03 02 09 72 01 8c 16 00 00 46 00 00 00 dd 1a
0110 00 50 f2 01 01 00 00 50 f2 02 02 00 00 50 f2 04
0120 00 50 f2 02 01 00 00 50 f2 02 30 18 01 00 00 0f
0130 ac 02 02 00 00 0f ac 04 00 0f ac 02 01 00 00 0f
0140 ac 02 00 00 dd 80 00 50 f2 04 10 4a 00 01 10 10
0150 44 00 01 02 10 3b 00 01 03 10 47 00 10 87 65 43
0160 21 9a bc de f0 12 34 50 d4 f7 81 32 d9 10 21 00
0170 07 54 50 2d 4c 69 6e 6b 10 23 00 09 41 72 63 68
0180 65 72 5f 41 39 10 24 00 03 31 2e 30 10 42 00 0c
0190 41 72 63 68 65 72 20 41 39 20 76 36 10 54 00 08
01a0 00 06 00 50 f2 04 00 01 10 11 00 0a 41 72 63 68
01b0 65 72 41 39 20 76 36 10 00 00 00 0a 41 72 63 68
```



**Thank you for
watching!!**



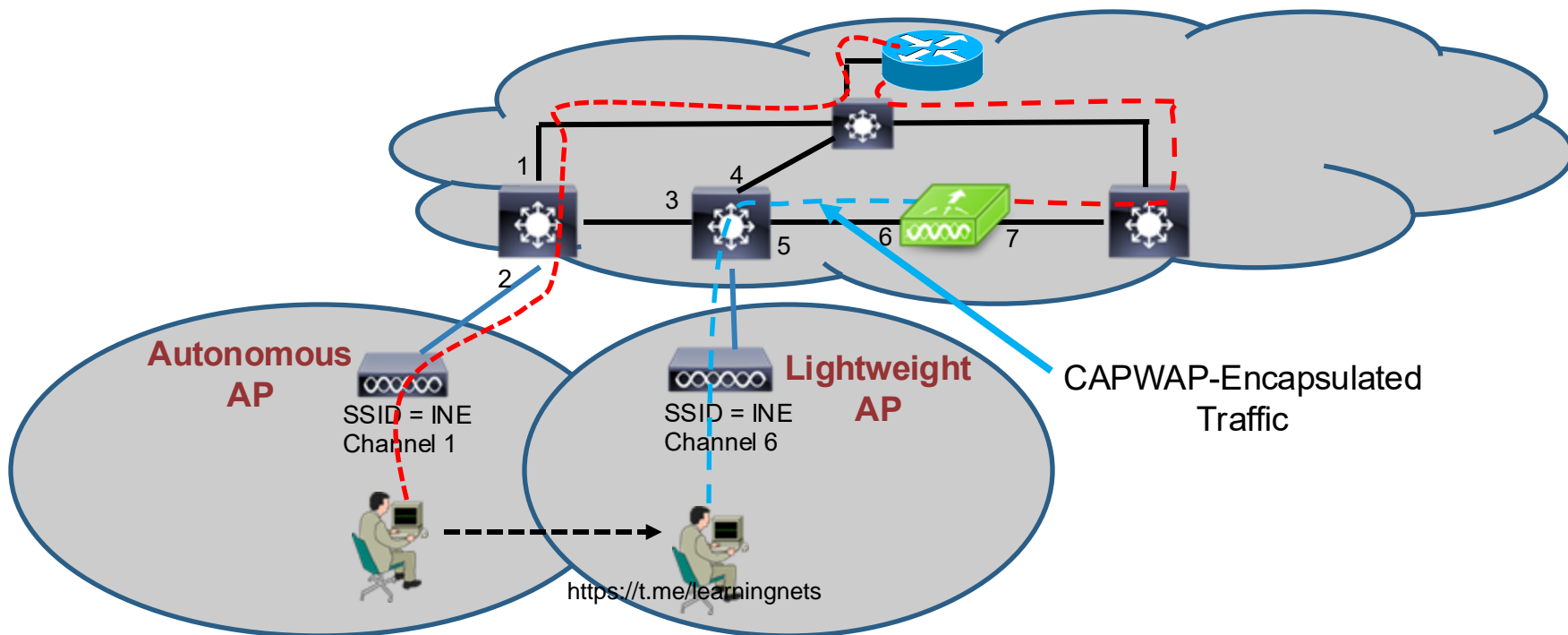
Categories of Wireless Roaming

Roaming Categories

- + For a WLAN client to “Roam” its IP address must be preserved.
- + Access points involved in a roaming event can be;
 - + Both Autonomous
 - + Both Lightweight
 - + A mixture
- + Roaming is characterized based on the presence, and quantity, of WLAN Controllers involved.

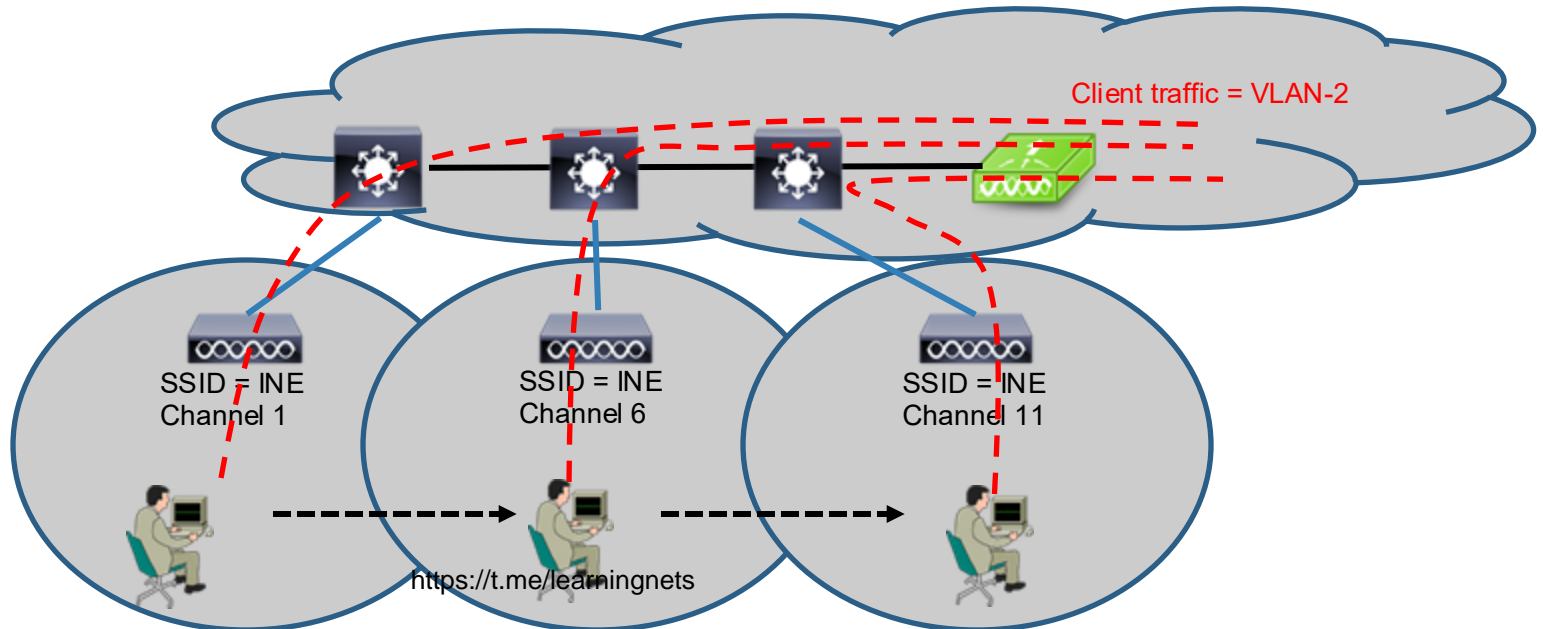
Autonomous Roam

- + Client roams to, or away from, an autonomous access point.
- + No elegant handoff between APs



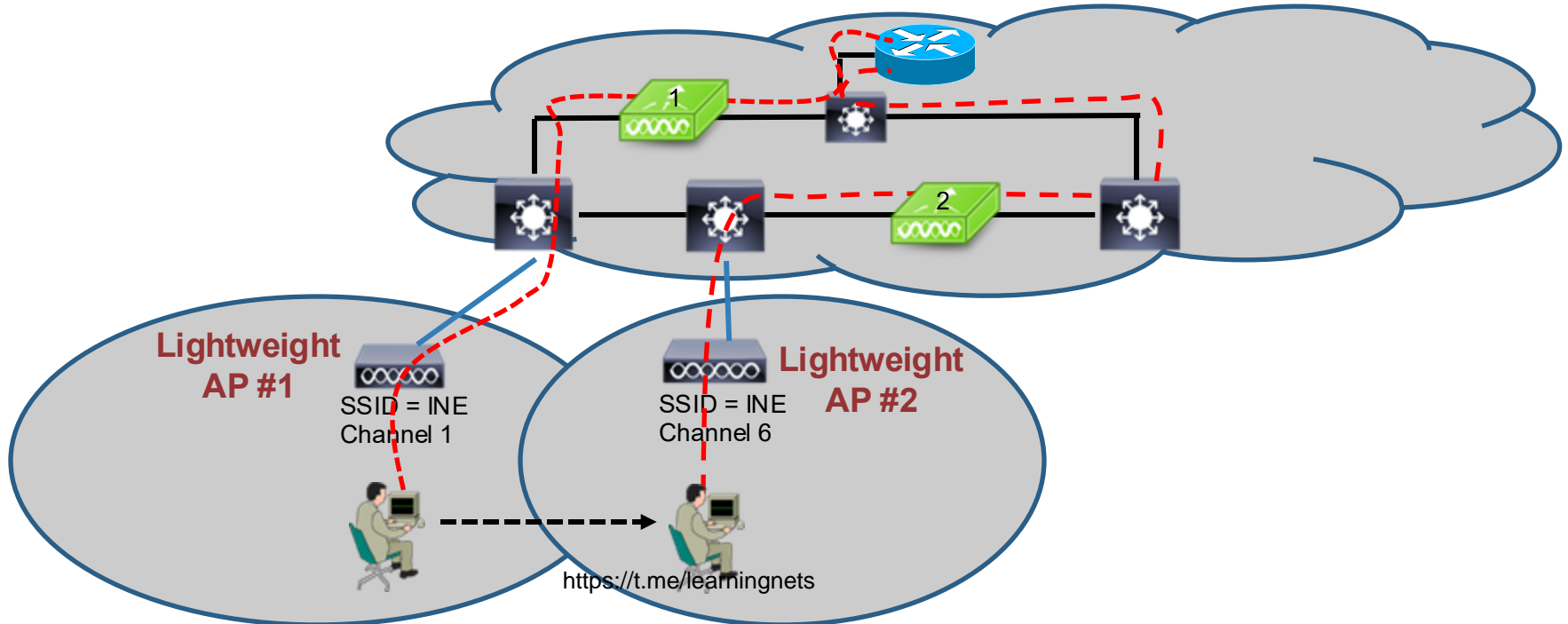
Intra-Controller Roam

- + Wi-Fi client roams between access points managed by the same WLAN controller



Inter-Controller Roam

- + WLAN client roams between access points managed by different WLAN controllers

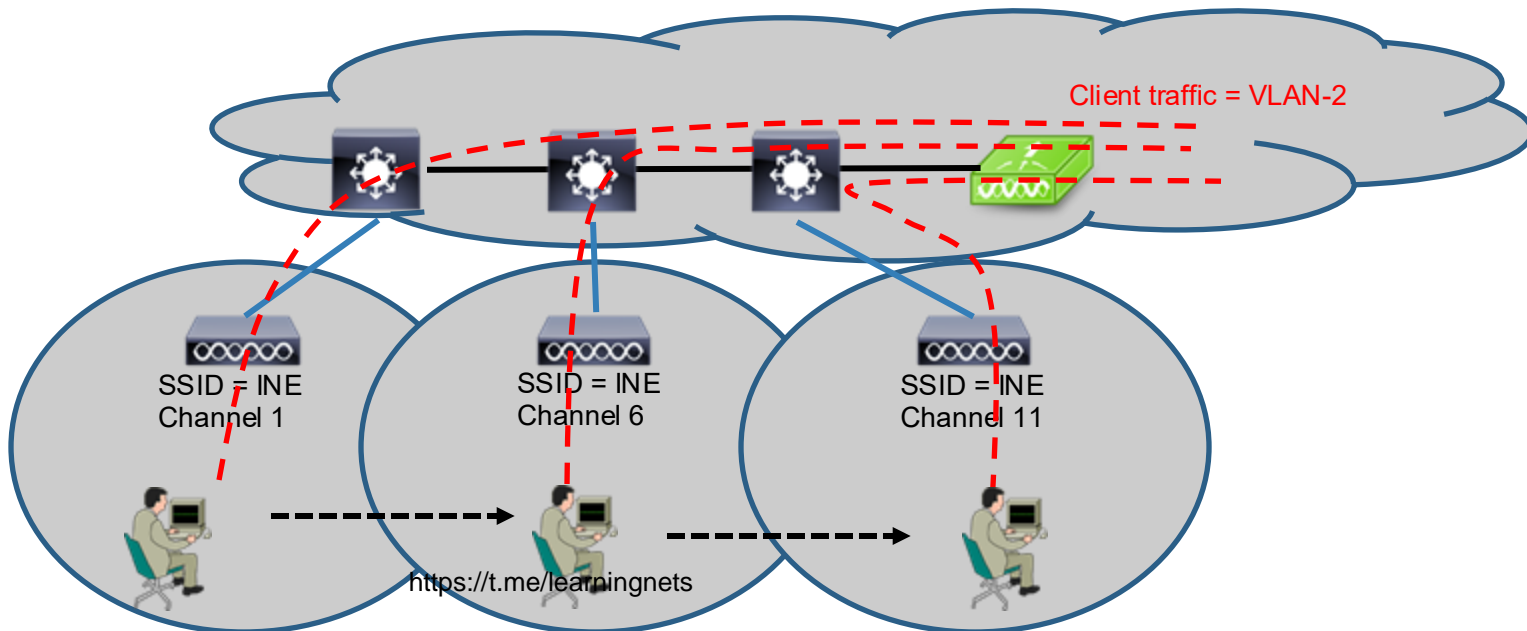


Layer-2 or Layer-3?

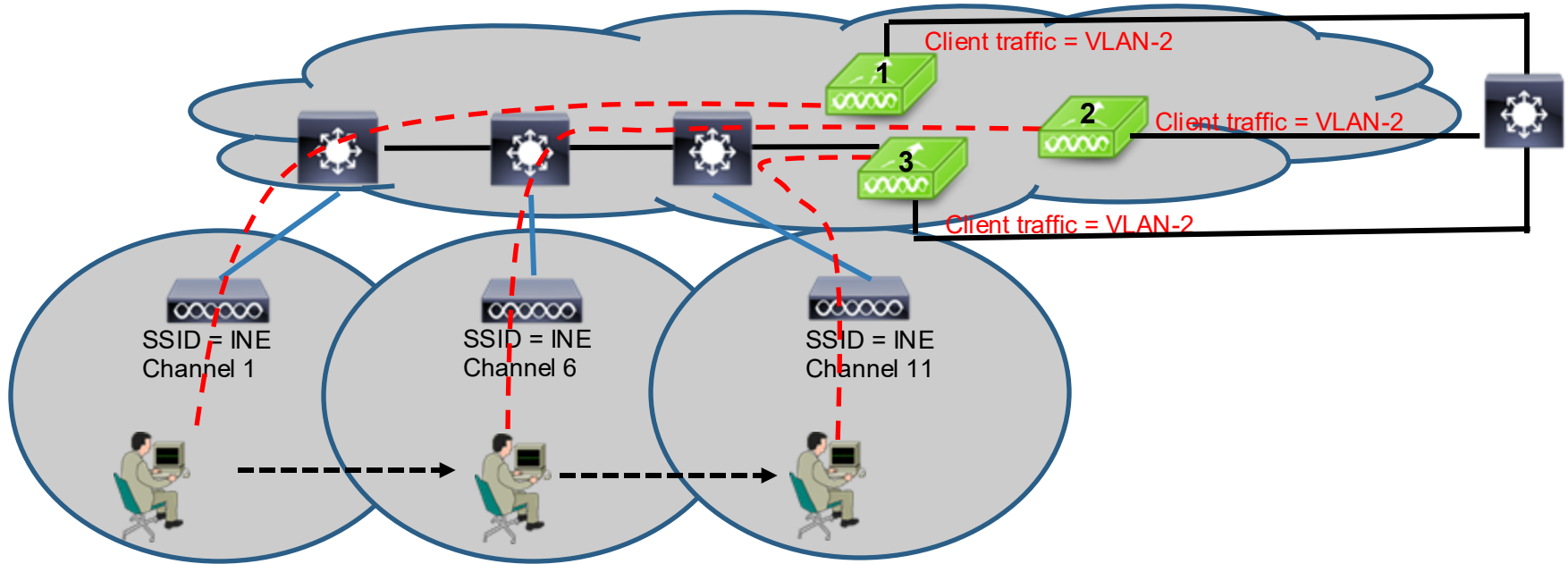
- + Inter-Controller roaming is also defined as either:
 - + Layer-2 roaming
 - + Layer-3 roaming
- + The controller's uplink mapping of SSID-to-VLAN is what makes the difference
 - + Two controllers, same SSID, same VLAN-to-SSID mapping = Layer-2 roam
 - + Two controllers, same SSID, different VLAN-to-SSID mapping = Layer-3 roam
- + In both cases, WLAN client IP address must be preserved to technically call it a "roam" event.

Layer-2 Roaming (Intra-Controller)

- + Wi-Fi client remains in the same IP subnet
- + Client's IP address is preserved
- + This type of roaming minimizes application downtime

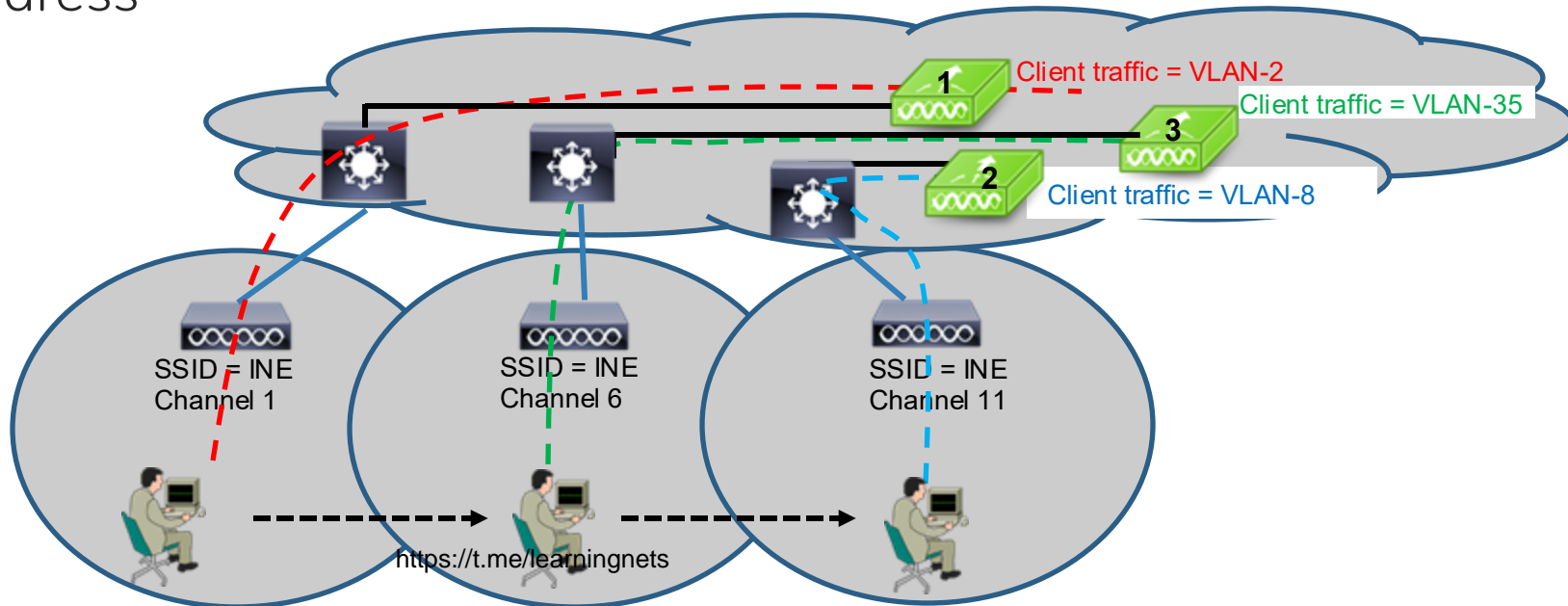


Layer-2 Roaming (Inter-Controller)



Layer-3 Roaming

- + BSS's have same SSID, but connect to different IP subnets on the wired network (Distribution System)
- + Requires tunneling techniques for Wi-Fi client to retain IP address





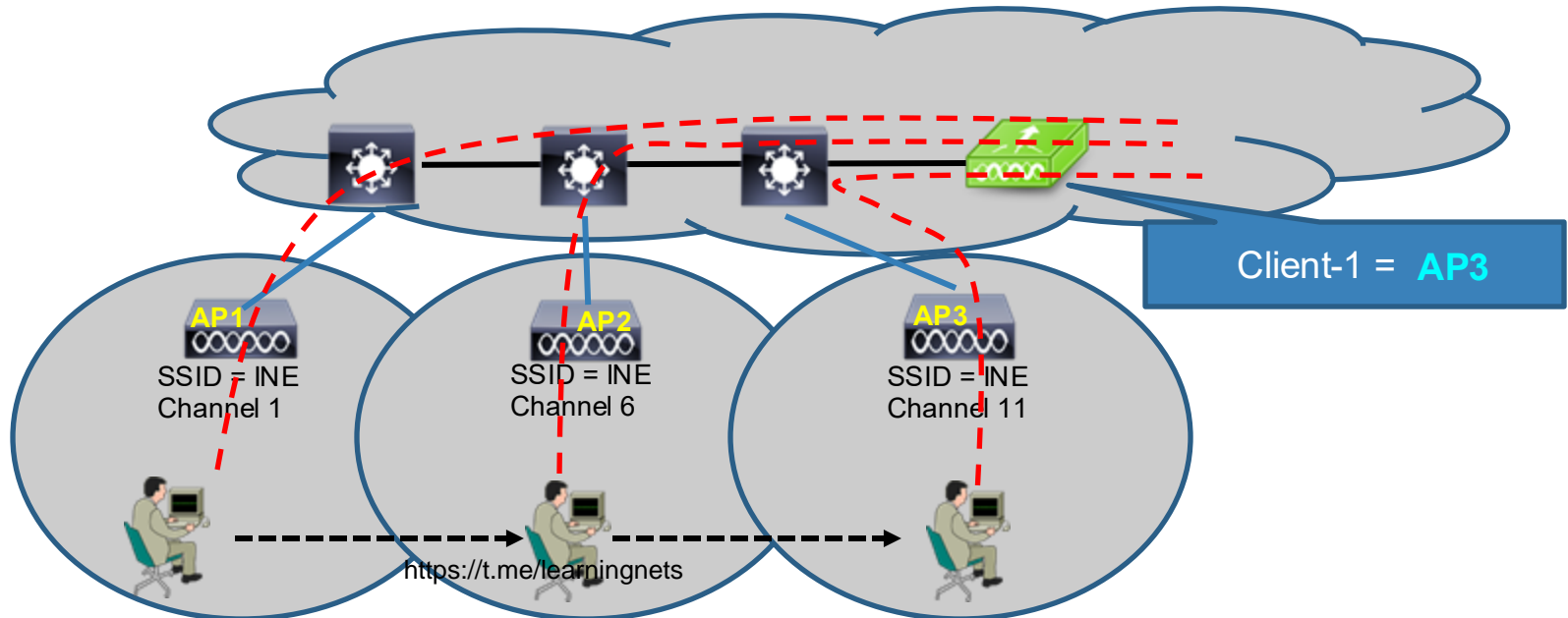
**Thank you for
watching!!**



Intra-Controller Roaming

Intracontroller Roaming

- + All access points have CAPWAP tunnels to a single WLC
- + WLC maintains list of client-to-AP mappings
- + WLC simply updates this list when a roaming event occurs

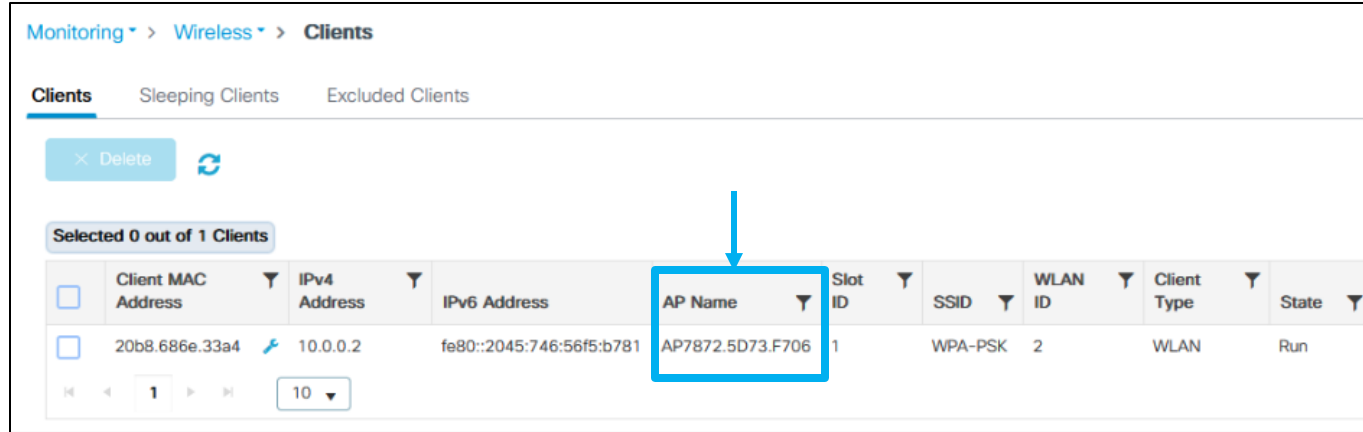


Controller Client Entries

- + When a wireless client associates/authenticates to an access point, the controller creates a client database entry
- + Entry includes:
 - + Client's MAC and IP addresses
 - + Security context and associations
 - + Quality of Service (QoS) contexts
 - + WLAN ID and associated access point
- + Controller uses this data to:
 - + Forward frames
 - + Manage traffic to/from the wireless client

Viewing Client Information

+ Before the roam...



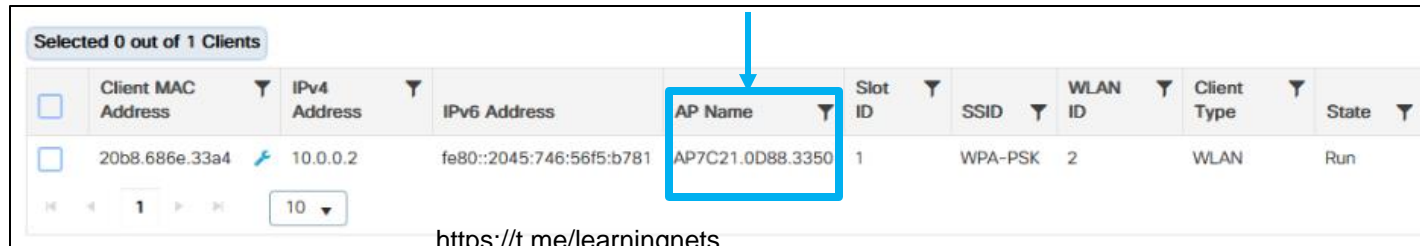
Monitoring > Wireless > Clients

Clients Sleeping Clients Excluded Clients

Selected 0 out of 1 Clients

<input type="checkbox"/>	Client MAC Address	IPv4 Address	IPv6 Address	AP Name	Slot ID	SSID	WLAN ID	Client Type	State
<input type="checkbox"/>	20b8.686e.33a4	10.0.0.2	fe80::2045:746:56f5:b781	AP7872.5D73.F706	1	WPA-PSK	2	WLAN	Run

+ After the roam...



Selected 0 out of 1 Clients

<input type="checkbox"/>	Client MAC Address	IPv4 Address	IPv6 Address	AP Name	Slot ID	SSID	WLAN ID	Client Type	State
<input type="checkbox"/>	20b8.686e.33a4	10.0.0.2	fe80::2045:746:56f5:b781	AP7C21.0D88.3350	1	WPA-PSK	2	WLAN	Run

<https://t.me/learningnets>

Notifying The Access Points

- + As a WLAN client reassociates (“roams”) to a new access point, 802.11 messages are exchanged which are all transmitted via CAPWAP to the WLC Controller
- + CAPWAP is also used by WLC to inform the “old” access point the client is no longer associated to it.

Using Radioactive Trace

Troubleshooting > Radioactive Trace

Conditional Debug Global State: **Stopped**

+ Add

× Delete

✓ Start

■ Stop

	MAC/IP Address	Trace file
<input type="checkbox"/>	20b8.686e.33a4	Generate

1 of 1 items

Last Run Result

✓ State	Successful See Details
MAC/IP Address	20b8.686e.33a4
Start Time	07/24/2025 20:27:59
End Time	07/24/2025 20:28:00
Trace file	debugTrace_20b8.686e.33a4.txt ↓

<https://t.me/learningnets>



Viewing the Roaming Handoff

```
*debugTrace_20b8.686e.33a4(2) - Notepad
File Edit Format View Help
Logging display requested on 2025/07/24 20:28:00 (EST) for Hostname: [WLC], Model: [C9800-CL-K9],
Version: [17.12.04], SN: [9NJPH5POVHT], MD_SN: [9NJPH5POVHT]

2025/07/24 20:27:23.515061415 {wncd_x_R0-0}{1}: [client-orch-sm] [14391]: (note): MAC: 20b8.686e.33a4
Re-Association received. BSSID 7872.5d75.9dce WLAN WPA-PSK, Slot 1 AP 7872.5d75.9dc0,
AP7872.5D73.F706, Site tag default-site-tag, Policy tag Roaming-Tag, Policy profile Roaming-Test,
Switching Central, old BSSID 7c21.0d89.09ee, Socket delay 0ms

2025/07/24 20:27:23.521576318 {wncd_x_R0-0}{1}: [dot11] [14391]: (note): MAC: 20b8.686e.33a4 Association
success. AID 1, Roaming = True, WGB = False, 11r = False, 11w = False Fast roam = False

2025/07/24 20:27:23.525899360 {wncd_x_R0-0}{1}: [client-orch-sm] [14391]: (note): MAC: 20b8.686e.33a4
Delete mobile payload sent for BSSID: 7c21.0d89.09ee WTP mac: 7c21.0d89.09e0 slot id: 1
```



**Thank you for
watching!!**



Cisco Catalyst 9800 Mobility Groups

Introduction to Mobility Groups

- + In Cisco terminology “Inter-Controller” roaming assumes the following;
 - + Two or more WLCs exist
 - + Those WLCs are managing different groups of APs
 - + WLANs and their settings are duplicated across Controllers
 - + Those WLCs are aware of each other and capable of sharing WLAN Client information
- + Mobility Groups must be configured to permit sharing of WLAN client information between WLCs

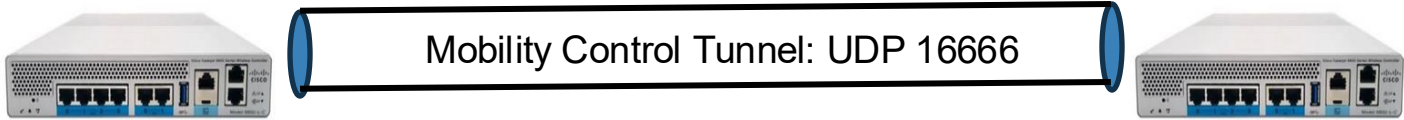
What are Mobility Groups?

- + A group of WLCs all sharing the same Mobility Group name
- + Allows WLCs to share WLAN Client & SSID information across mobility tunnels
- + Can have up to 8-controllers in a Mobility Group
- + Requires a full-mesh of connections between controllers
- + Multicast can be used for large groups

Mobility Tunnels Overview

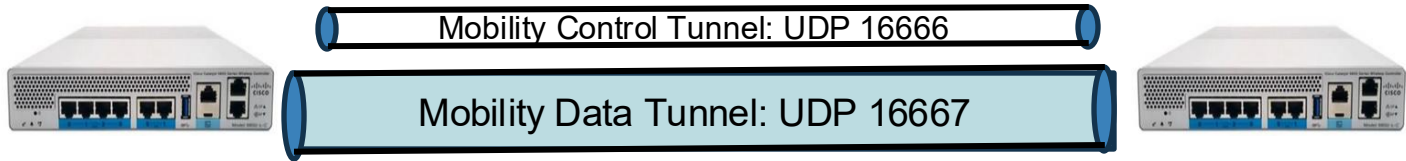
- + Mobility peering creates UDP-based mobility tunnels between peers:
 - + Mobility Control Tunnel
 - + UDP port 16666
 - + Implements DTLS encryption
 - + Mobility Data Tunnel
 - + UDP port 16667
 - + Can be optionally configured for DTLS encryption

Mobility Control Tunnels



- + Mobility Control Messages
- + Heartbeats
- + Client Session Synchronization
- + Messages for optional fast roaming techniques
 - + Fast Transition (FT) Control Messages
 - + OKC (Opportunistic Key Caching) Control Messages

Mobility Data Tunnels



- + Client data frames during Layer-3 roams
- + Fast Transition (FT) pre-authentication data PDUs
- + Diagnostic/Monitoring traffic
- + Keepalive Packets: Periodic small packets to ensure the tunnel remains operational.

Mobility Global Configuration

Configuration > Wireless > Mobility

Global Configuration Peer Configuration

Mobility Group Name*	default
Multicast IPv4 Address	0.0.0.0
Multicast IPv6 Address	::
Keep Alive Interval (sec)*	10
Mobility Keep Alive Count*	3
Mobility DSCP Value*	48
Mobility MAC Address	001e.bd9c.18ff
DTLS High Cipher Only* ⓘ	<input type="checkbox"/> DISABLED

There is no need to change any of these values.

<https://t.me/learningnets>



Mobility Peer Configuration (1)

Configuration > Wireless > Mobility

Global Configuration Peer Configuration

▼ Mobility Peer Configuration

+ Add **× Delete**

MAC Address	IP Address	Public IP	Group Name	SSC Hash	Data Link Encryption
001e.bd9c.18ff	10.199.199.254	N/A	default	5fb51870fa2dce965dfef253e3c775067eec09fb	N/A

1 - 1 of 1 items

This is information about your local WLC. Some of these values will be configured on the remote peer.

Mobility Peer Configuration (2)

The screenshot shows the 'Add Mobility Peer' configuration window with the following fields and values:

- MAC Address*: 001e.7aba.01ff
- Peer IPv4/IPv6 Address*: 10.199.199.250 (with a 'Ping Test' button)
- Public IPv4/IPv6 Address: (empty field)
- Group Name*: default
- Data Link Encryption: default
- SSC Hash: 7c4690a9e5987f2d1455034c062ab1b3b04

Annotations:

- A red arrow points from the 'Public IPv4/IPv6 Address' field to a callout box: "Publicly-reachable address of peer across a NAT network." The word "Optional" is written in red above the box.
- A red arrow points from the 'SSC Hash' field to a callout box: "Only if peering with 9800-CL". The word "Optional" is written in red above the box.

Buttons: Cancel, Apply to Device

Mobility Peer Verification

Configuration > Wireless > Mobility

Global Configuration Peer Configuration

▼ Mobility Peer Configuration

+ Add × Delete ↻

	MAC Address ▼	IP Address ▼	Public IP ▼	Group Name
	001e.bd9c.18ff	10.199.199.254	N/A	default
<input type="checkbox"/>	001e.7aba.01ff	10.199.199.250	10.199.199.250	default

...

Status ▼
N/A
Up



**Thank you for
watching!!**

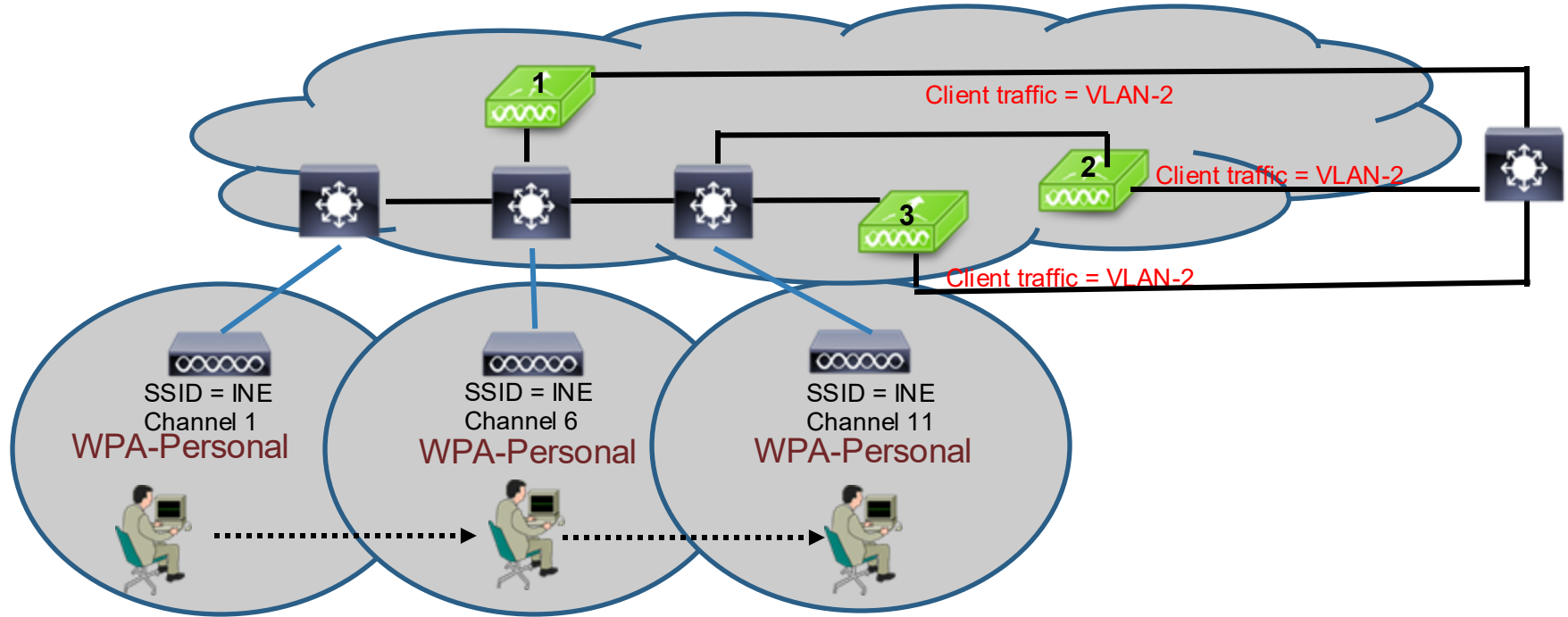


Contrasting Mobility Group Performance

Not Always Necessary

- + Under some circumstances, mobility groups aren't needed;
 - + Both WLCs are configured for the same WLAN
 - + WLAN is mapped to same VLAN on both controllers
 - + Both controllers have an uplink carrying that VLAN
 - + Ideally, WLAN is utilizing WPA PSK (not 802.1x)
- + Let's see an example of this...

No Mobility Needed



PSK Inter-Controller Roam

- + No mobility groups have been configured

Post-Roam
(on 9800-2)

Monitoring > Wireless > Clients

Clients Sleeping Clients Excluded Clients

Selected 0 out of 1 Clients

<input type="checkbox"/>	Client MAC Address	IPv4 Address	IPv6 Address	AP Name	Slot ID	SSID	WLAN ID	Client Type	State
<input type="checkbox"/>	20b8.686e.33a4	10.0.0.1	fe80::2045:746:56f5:b781	<u>AP7C21.0D88.3350</u>	1	WPA-PSK	1	WLAN	Run

Pre-Roam
(on 9800-1)

Configuration >

Administration >

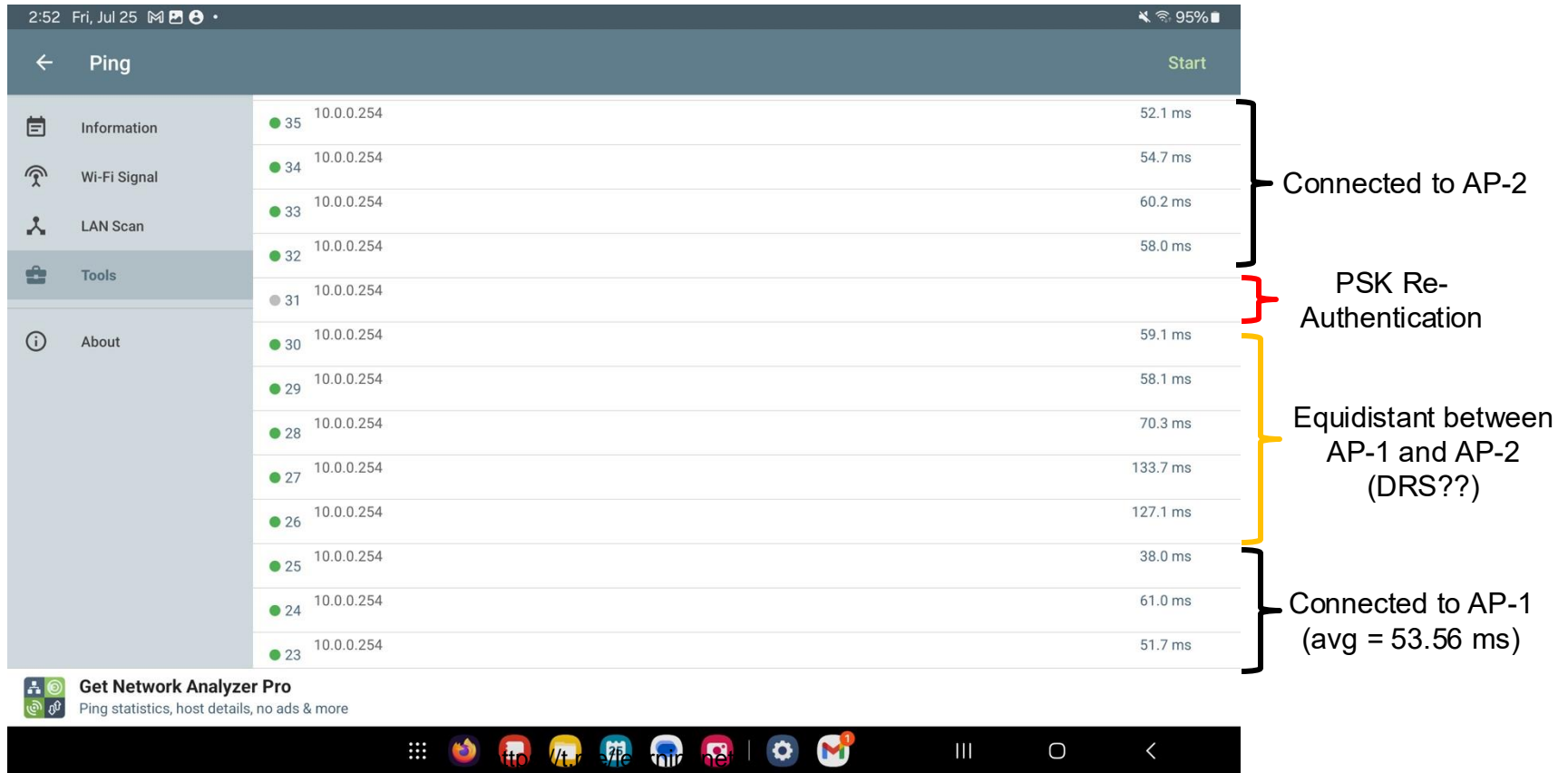
Licensing

Selected 0 out of 1 Clients

<input type="checkbox"/>	Client MAC Address	IPv4 Address	IPv6 Address	AP Name	Slot ID	SSID	WLAN ID
<input type="checkbox"/>	20b8.686e.33a4	10.0.0.1	fe80::2045:746:56f5:b781	<u>AP7872.5D73.F706</u>	1	WPA-PSK	2

<https://t.me/learningnets>

PSK Inter-Controller Roam



802.1x Inter-Controller Roam

+ No Mobility Groups have been configured

Post-Roam
9800-2

Monitoring > Wireless > Clients

Clients Sleeping Clients Excluded Clients

Selected 0 out of 1 Clients

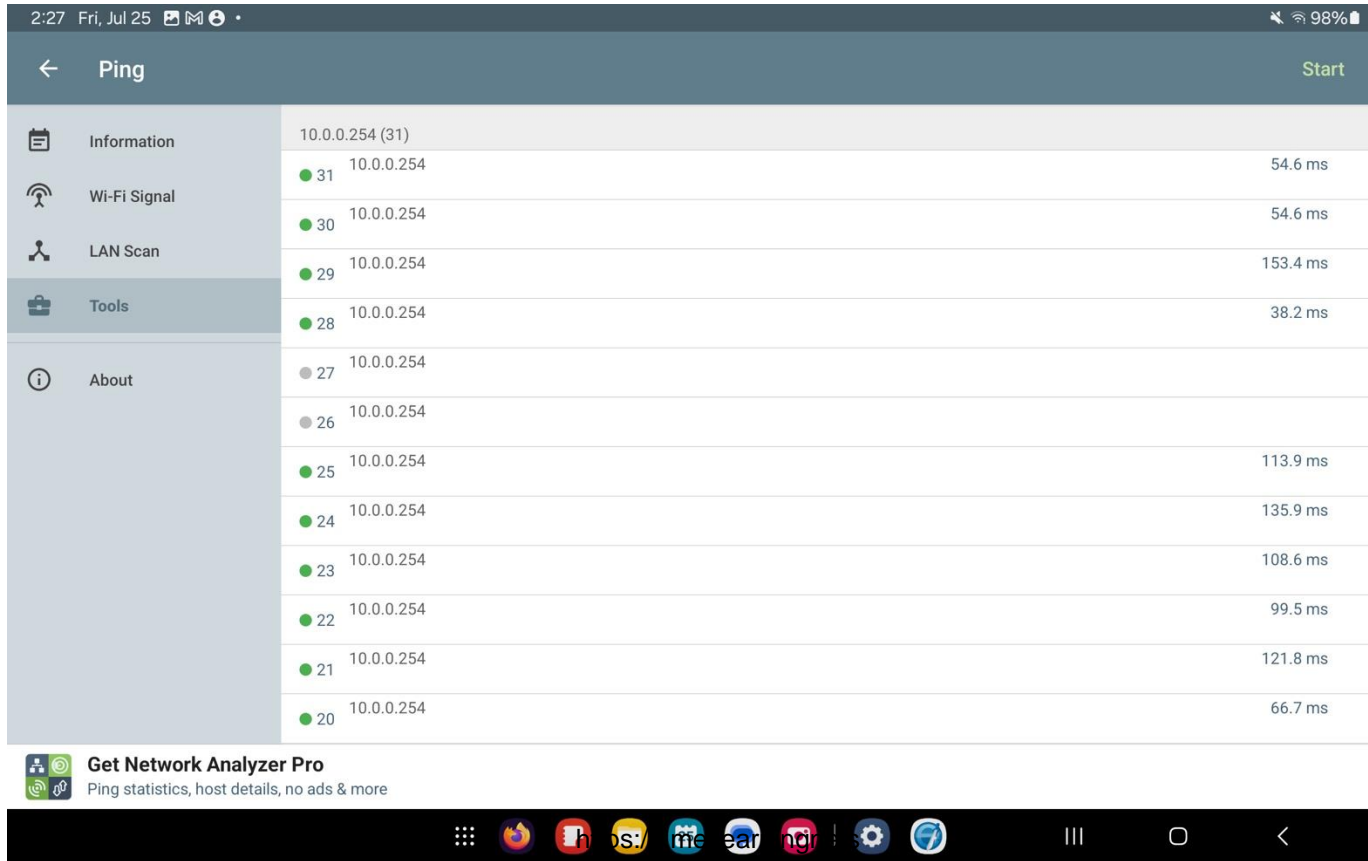
<input type="checkbox"/>	Client MAC Address	IPv4 Address	IPv6 Address	AP Name	Slot ID	SSID	WLAN ID	Client Type
<input type="checkbox"/>	daff.ce28.22b8	10.0.0.2	fe80::d8ff:ceff:fe28:22b8	<u>AP7C21.0D88.3350</u>	1	Dot1x-Test	2	WLAN

Pre-Roam
9800-1

Selected 0 out of 1 Clients

<input type="checkbox"/>	Client MAC Address	IPv4 Address	IPv6 Address	AP Name	Slot ID	SSID	WLAN ID	Client Type
<input type="checkbox"/>	daff.ce28.22b8	10.0.0.2	fe80::d8ff:ceff:fe28:22b8	<u>AP7872.5D73.F706</u>	1	Dot1x-Test	1	WLAN

802.1x Data Loss without Mobility Group



WPA PSK Roaming **WITH** Mobility Tunnel

The screenshot shows a mobile application interface with a dark theme. At the top, the status bar displays the time 3:50, the date Fri, Jul 25, and a battery level of 92%. The app's main header is titled "Ping" with a back arrow on the left and a "Start" button on the right. A sidebar menu on the left contains several options: Information, Wi-Fi Signal, LAN Scan, Tools (which is currently selected), and About. The main content area displays a list of ping results for the IP address 10.0.0.254. Each entry consists of a green dot with a number (ranging from 12 to 24), the IP address, and the response time in milliseconds. At the bottom of the screen, there is a promotional banner for "Get Network Analyzer Pro" and a dock with various system and app icons.

Count	IP Address	Response Time (ms)
24	10.0.0.254	42.6 ms
23	10.0.0.254	42.3 ms
22	10.0.0.254	88.8 ms
21	10.0.0.254	54.6 ms
20	10.0.0.254	79.6 ms
19	10.0.0.254	105.8 ms
18	10.0.0.254	47.8 ms
17	10.0.0.254	56.6 ms
16	10.0.0.254	58.9 ms
15	10.0.0.254	52.9 ms
14	10.0.0.254	51.6 ms
13	10.0.0.254	50.9 ms
12	10.0.0.254	51.5 ms

Get Network Analyzer Pro
Ping statistics, host details, no ads & more



802.1x Roaming **WITH** Mobility Tunnel

The screenshot shows a mobile application interface for network diagnostics. The top status bar displays the time as 3:56 on Friday, July 25, with a battery level of 91%. The app title is "Ping" and it includes a "Start" button in the top right corner. A sidebar menu on the left contains options: Information, Wi-Fi Signal, LAN Scan, Tools, and About. The main content area is a list of ping results for the IP address 10.0.0.254. Each entry includes a ping number (from 29 to 41), the IP address, and the response time in milliseconds. The entry for ping number 36 is highlighted with a red rectangular box. At the bottom of the screen, there is an advertisement for "Get Network Analyzer Pro" and an Android navigation bar with various app icons.

Ping #	IP Address	Response Time (ms)
41	10.0.0.254	41.3 ms
40	10.0.0.254	33.9 ms
39	10.0.0.254	33.3 ms
38	10.0.0.254	54.2 ms
37	10.0.0.254	155.1 ms
36	10.0.0.254	150.6 ms
35	10.0.0.254	124.6 ms
34	10.0.0.254	118.4 ms
33	10.0.0.254	149.4 ms
32	10.0.0.254	53.4 ms
31	10.0.0.254	51.6 ms
30	10.0.0.254	55.2 ms
29	10.0.0.254	

Get Network Analyzer Pro
Ping statistics, host details, no ads & more



Benefits of Mobility Groups

- + Roaming is much faster with Mobility Groups under the following conditions:
 - + Layer-3 inter-controller roaming
 - + Roaming that utilizes fast transition mechanisms
- + Rule of thumb – Just configure it, when implementing two or more controllers

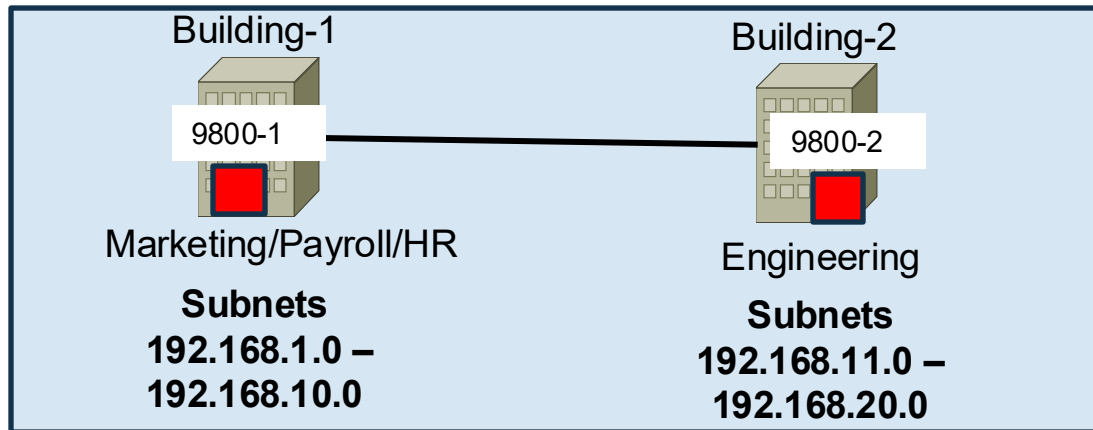


**Thank you for
watching!!**



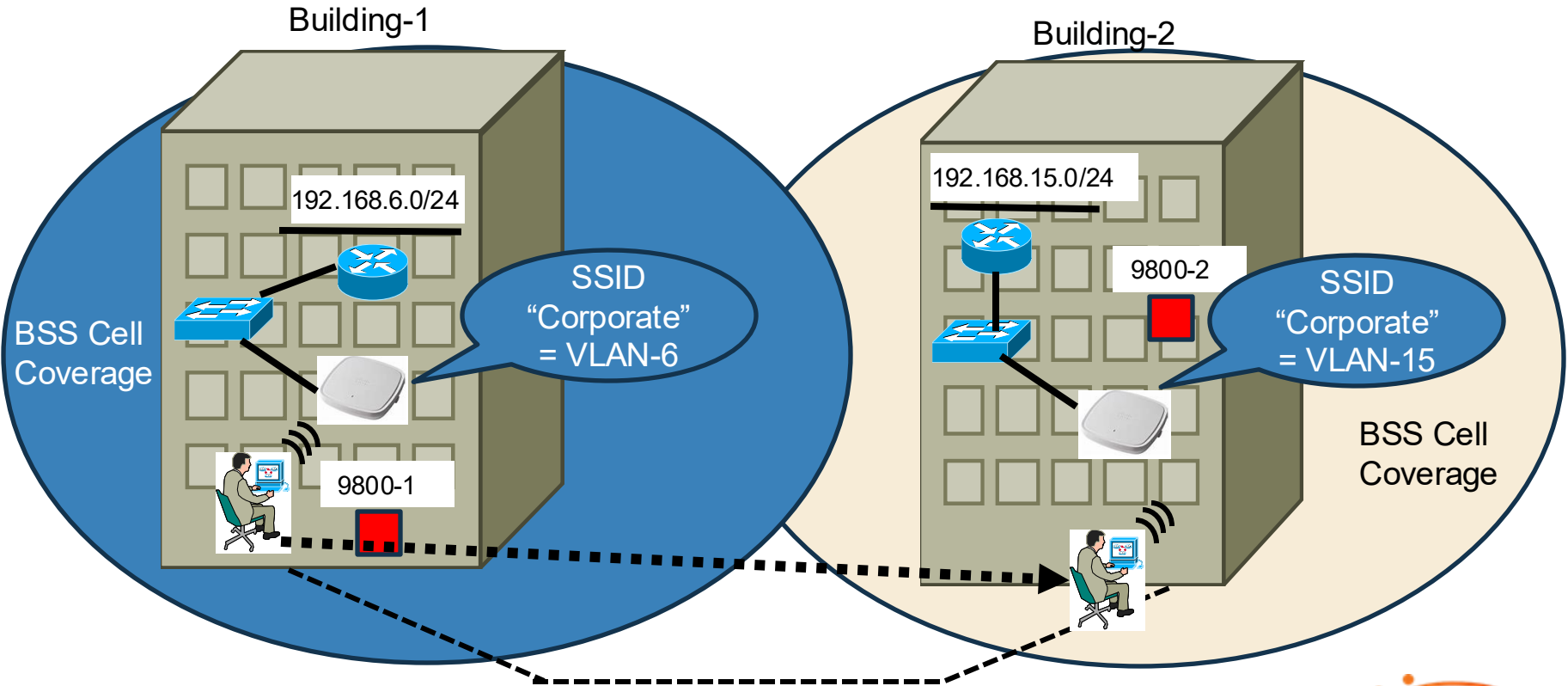
Layer-3 Inter-Controller Roaming

A Design Scenario



- + Each building has its own Cisco 9800 WLC managing multiple access points.
- + Employees should be able to connect to SSID, “Corporate” in either building
- + Employees should be able to roam within, and between buildings (retain IP addresses)

The Problem



<http://www.inegroup.com>



Layer-3 Inter-Controller Roaming

- + This type of roaming requires the following:
 - + WLCs connected by a Mobility Group
 - + Identical WLANs advertised by each WLC with the exception of VLAN assignment
 - + Implementation of “Anchor” and “Foreign” roles on WLCs

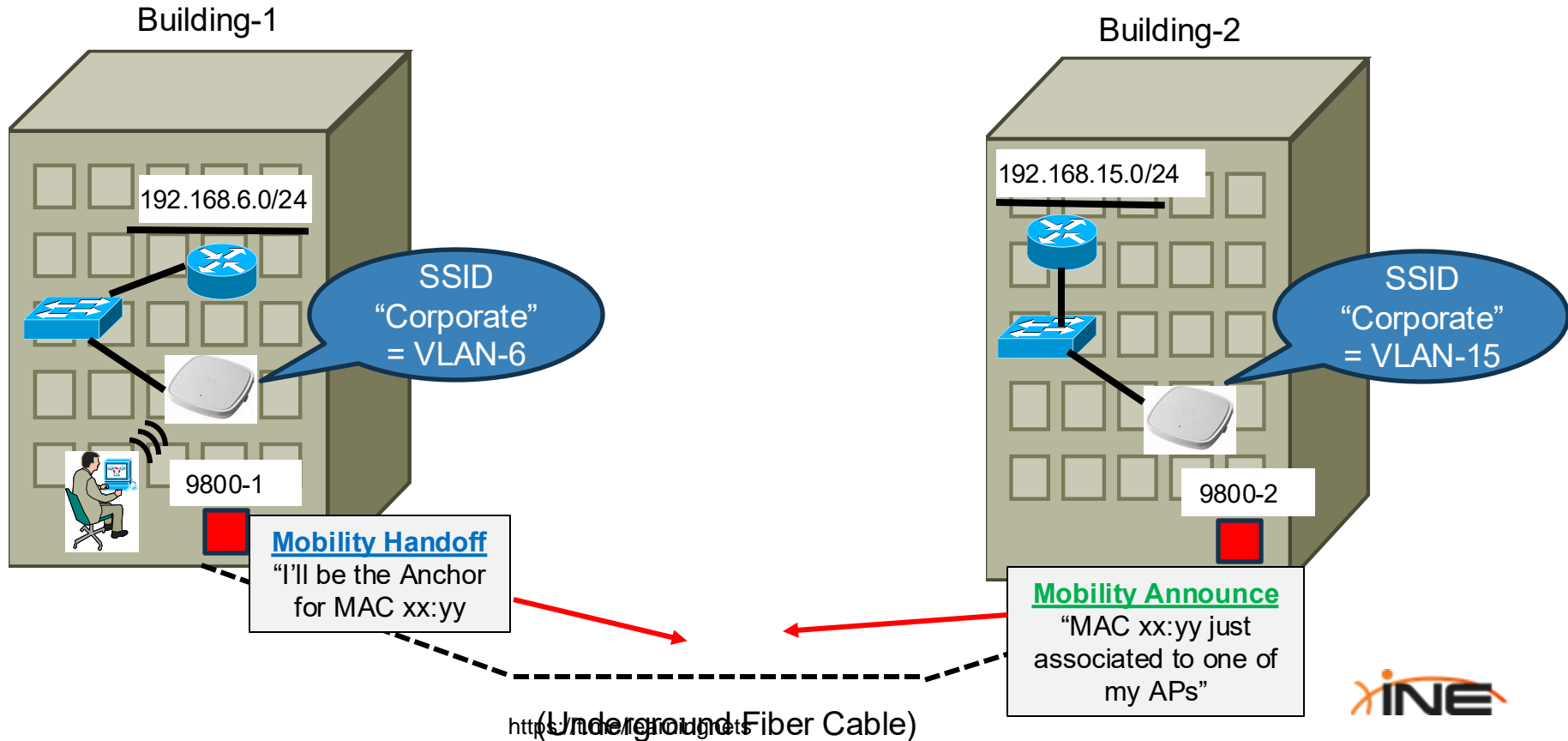
Anchor & Foreign

- + Anchor Controller: Automatic designation given when client sends an “Association Request” message
- + Foreign Controller: Role that a controller takes when:
 - + It receives a WLAN client “Reassociation Request”
 - + Discovers the client was previously managed by a different 9800 controller
 - + Learns that the client is trying to attempt a Layer-3 roam.
- + No configuration needed (other than Mobility Groups) for these roles to be assigned.

Anchor & Foreign

- + Anchor continues switching traffic into the distribution system (wired network)
- + The client entry exists on both controllers:
 - + Marked as “Anchor” on the original controller (where the client first connected)
 - + Marked as “Foreign” on the controller the client roamed to
- + Client maintains its original IP address, while the Anchor handles traffic insertion into the network and the Foreign handles client association locally

L3 Roaming Mobility Messages



The Anchor's Perspective

- + Upon first association to an access point...

The screenshot shows a network management interface with the following elements:

- Navigation: Monitoring > Wireless > Clients
- Tabs: Clients (selected), Sleeping Clients, Excluded Clients
- Buttons: Delete, Refresh
- Status: Selected 0 out of 1 Clients
- Table with columns: Client MAC Address, IPv4 Address, IPv6 Address, AP Name, Slot ID, SSID, WLAN ID, Client Type, Role
- Client Data Row: 20b8.686e.33a4, 20.0.0.2, fe80::2045:746:56f5:b781, 10.199.199.254, 255, WPA-PSK, 2, WLAN, Anchor
- Footer: 1 - 1 of 1

Red annotations in the image include a box around the 'AP Name' and 'Slot ID' columns and a circle around the 'Anchor' role in the dropdown menu.

- + After performing a Layer-3 inter-controller roam, client is still visible on “Anchor” controller
- + “AP Name” changes to WMI of foreign controller

The Foreign Perspective

Monitoring > Wireless > Clients

Clients Sleeping Clients Excluded Clients

× Delete



Selected 0 out of 1 Clients

<input type="checkbox"/>	Client MAC Address	IPv4 Address	IPv6 Address	AP Name	Slot ID	SSID	...
<input type="checkbox"/>	20b8.686e.33a4	20.0.0.2	fe80::2045:746:56f5:b781	AP7872.5D73.F706	1	WPA-PSK	...

Role

Foreign

1 - 1 of

Monitoring Mobility (9800)

Monitoring > Wireless > Mobility

Join Statistics		Roam Statistics	
Local	0	L2 roam count	0
Foreign	0	L3 roam count	1
Export Foreign	0	Flex client roam count	0
Export Anchor	0	Inter-WNCd roam count	0
Delete Statistics		Intra-WNCd roam count	0
Local	0	Remote Web Auth Pending Roams	0
Remote	0		
Role Change Statistics			
Local to Anchor	1		
Anchor to Local	0		

One client associated to this controller, then performed a L3 roam away from it.

Monitoring Mobility (9800)

Client associated to anchor controller, then performed a L3 roam to this “Foreign” controller.

Monitoring > Wireless > Mobility

Join Statistics	
Local	0
Foreign	1
Export Foreign	0
Export Anchor	0

Delete Statistics	
Local	0
Remote	0

Role Change Statistics	
Local to Anchor	0
Anchor to Local	0

Roam Statistics	
L2 roam count	0
L3 roam count	1
Flex client roam count	0
Inter-WNCd roam count	0
Intra-WNCd roam count	0
Remote Web Auth Pending Roams	0

Monitoring Client Mobility History

Monitoring -> Wireless -> Clients

Recent association history:

AP Name	BSSID	AP Slot	Assoc Time	Instance	Mobility Role	Run Latency (ms)	Roam Type
AP7872.5D73.F706	7872.5d75.9dcf	1	07/29/2025 19:53:32	0	Local	203	802.11i Slow
10.199.199.250	0000.0000.0000	N/A	07/29/2025 19:50:20	0	Anchor	0	N/A
AP7872.5D73.F706	7872.5d75.9dcf	1	07/29/2025 19:49:12	0	Local	5540	N/A



**Thank you for
watching!!**



Roaming Latency Factors

<https://t.me/learningnets>



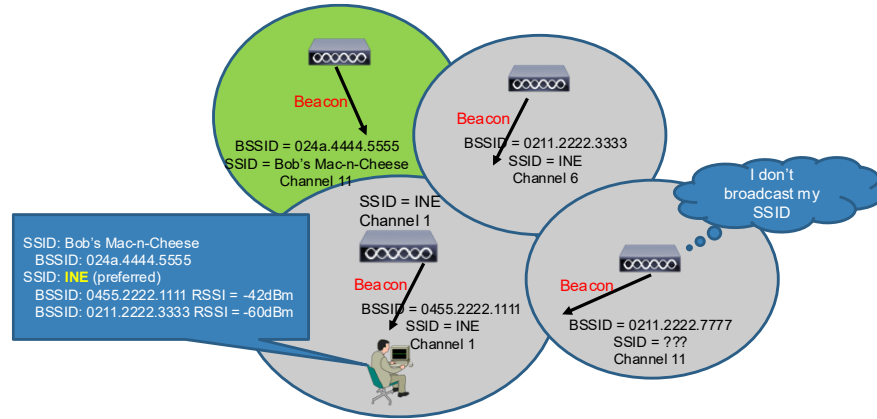
General Factors That Affect Roaming

- + Ideally, roaming will be fast (less than 50ms)
- + Multiple factors can delay this time;
 - + Client stickiness
 - + Time taken to discover a new access point
 - + Time taken to perform authentication
- + Not much can be done for the first issue, but solutions exist for the other two issues.

Roaming Impact on Delay-Sensitive Applications

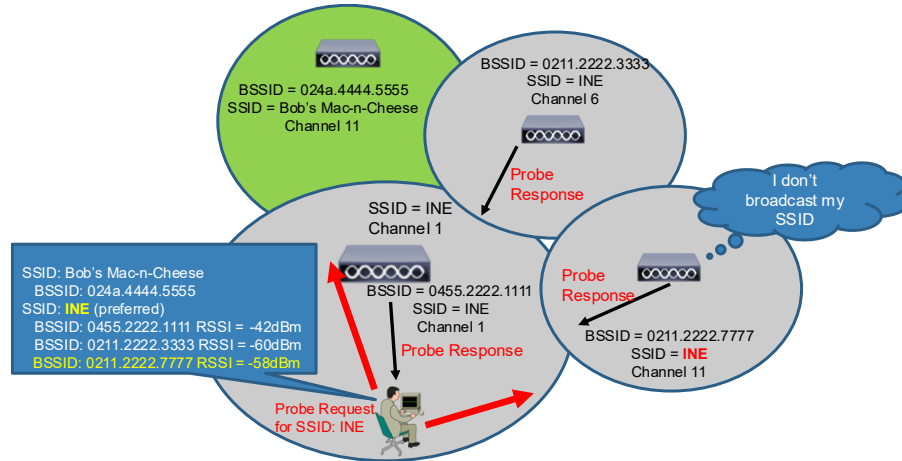
- + Delay-sensitive apps (e.g., voice, timeout-sensitive apps) may experience issues during roaming
- + User may perceive:
 - + Audio gaps
 - + Application disconnects
 - + Pauses in video
- + Severity depends on how quickly the client resumes sending/receiving data

Passive Scanning



- + Client dwells on all available channels, waiting for beacons
- + Benefit: Less battery consumption as this is receive-only
- + **Drawbacks:**
 - + Beacons typically transmitted roughly every 100ms
 - + Can take significant time to find all relevant beacons for desired SSID
 - + Hidden SSIDs are not discoverable

Active Scanning



- + Client transmits Probe Requests on every available channel
- + Benefit: Client doesn't have to wait for Beacons
- + **Drawbacks:**
 - + Consumes more client battery power
 - + Wastes time sending Requests on channels that don't have any relevant access points

Other Contributing Factors

- + Roaming delay duration influenced by:
 - + RF environment quality
 - + Number of clients
 - + Round-trip time between WLC, APs, and authentication server



**Thank you for
watching!!**



Cisco Compatibility Extensions (CCX)

<https://t.me/learningnets>



What is CCX?

- + Cisco Compatibility Extensions (CCX) = Cisco's proprietary Wi-Fi client enhancement framework
- + Extends standard 802.11 for better roaming, security, diagnostics, and QoS
- + Must be licensed and implemented by Wi-Fi client manufacturers
- + Versions: CCXv1 to CCXv5 (CCXv4/v5 most feature-rich)
 - + CCXv5 released in 2009
 - + CCX no longer supported by Cisco

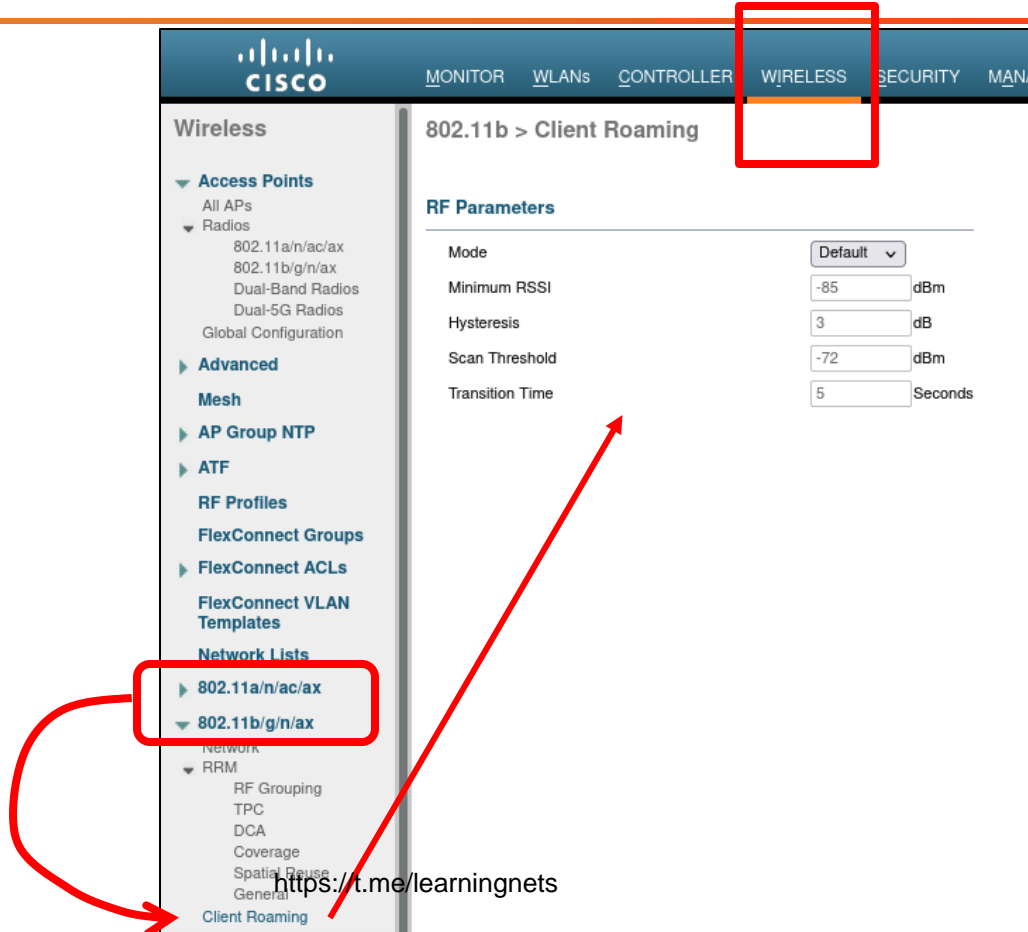
What Problem Does CCX Solve?

- + Slow or unreliable Wi-Fi roaming
- + VoIP call drops during AP transitions
- + Inconsistent performance with standard roaming (esp. in large or fast-moving environments)
- + Lack of visibility/telemetry from Wi-Fi clients in enterprise networks

How Did CCX Solve It?

- + Previous generations of Cisco WLAN controllers allowed one to tune CCX parameters (advertised to clients in access point Beacons) such as;
 - + Roaming Thresholds
 - + Scanning Thresholds
- + CCX also provided features such as;
 - + Enhanced Neighbor Lists
 - + Directed Roam Requests

Legacy CCX Roaming Threshold Configuration



Wireless

- Access Points
 - All APs
 - Radios
 - 802.11a/n/ac/ax
 - 802.11b/g/n/ax
 - Dual-Band Radios
 - Dual-5G Radios
 - Global Configuration
 - Advanced
 - Mesh
 - AP Group NTP
 - ATF
 - RF Profiles
 - FlexConnect Groups
 - FlexConnect ACLs
 - FlexConnect VLAN Templates
 - Network Lists
 - 802.11a/n/ac/ax
 - 802.11b/g/n/ax
 - Network
 - RRM
 - RF Grouping
 - TPC
 - DCA
 - Coverage
 - Spatial Reuse
 - General
 - Client Roaming

802.11b > Client Roaming

RF Parameters

Mode	Default
Minimum RSSI	-85 dBm
Hysteresis	3 dB
Scan Threshold	-72 dBm
Transition Time	5 Seconds

Who Uses CCX?

- + Not common in consumer laptops, phones, or tablets
- + Used in enterprise, industrial, or mission-critical clients
 - + Voice-over-Wi-Fi phones
 - + Warehouse barcode scanners
 - + Medical devices
 - + Ruggedized PDAs and mobile terminals

Examples of CCX-Enabled Clients

Manufacturer	Product Type	CCX Use Case
Motorola/Symbol	Barcode scanners (e.g. MC92N0)	Fast roaming in warehouses
Spectralink	Wi-Fi phones (e.g. 8400 Series)	Seamless voice mobility
Various OEMs	Industrial handhelds & PDAs	Inventory, logistics, healthcare



**Thank you for
watching!!**



Discover Your Neighbors with 802.11k

<https://t.me/learningnets>



Introduction to 802.11k

- + IEEE amendment focused on *assisting client roaming decisions*
- + Works in tandem with 802.11r (fast transition) and 802.11v (network steering)
- + Reduces roaming latency for mobile and latency-sensitive clients
- + Especially valuable in dense AP deployments such as enterprise or education environments

Historical Background

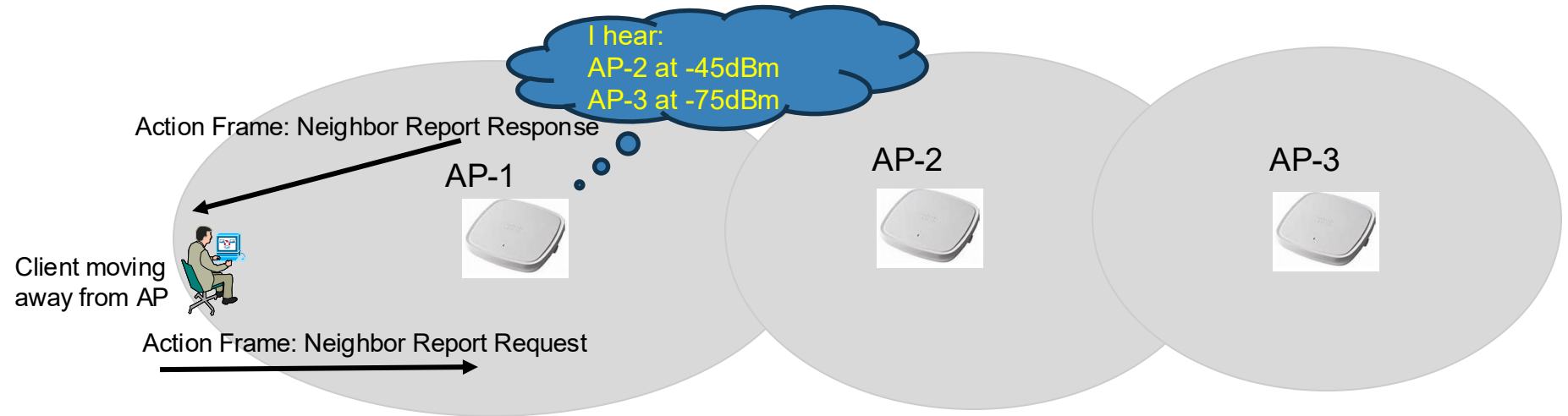
- + IEEE first begins working on 802.11k in 2006
- + Finalized and ratified as an official standard in 2008
- + Gained traction after adoption by Wi-Fi Alliance's Voice-Enterprise certification
- + Included in modern Wi-Fi chipsets and supported in Wi-Fi 4, 5, 6, and 6E clients

Optimizing AP Discovery with 802.11k

- + *802.11k-enabled APs provide clients with a neighbor report* (list of nearby APs)
- + Clients use this report to reduce scanning time
- + Enables informed roaming to optimal APs based on signal strength and load
 - + Scanning only required for channels included in the Neighbor List Report

802.11k Frame Exchange

- + *802.11k relies on the exchange of 802.11 “Action” management frame types*



Neighbor List Requests



```
> 802.11 radio information
v IEEE 802.11 Action, Flags: .....TC
  Type/Subtype: Action (0x000d)
  > Frame Control Field: 0xd001
    .000 0000 0011 1100 = Duration: 60 microseconds
  > Receiver address: Cisco_75:9d:cf (78:72:5d:75:9d:cf)
  > Destination address: Cisco_75:9d:cf (78:72:5d:75:9d:cf)
  > Transmitter address: 0a:c2:08:38:9d:b5 (0a:c2:08:38:9d:b5)
  > Source address: 0a:c2:08:38:9d:b5 (0a:c2:08:38:9d:b5)
  > BSS Id: Cisco_75:9d:cf (78:72:5d:75:9d:cf)
  > STA address: 0a:c2:08:38:9d:b5 (0a:c2:08:38:9d:b5)
    .... 0000 = Fragment number: 0
    0011 1100 1001 .... = Sequence number: 969
    Frame check sequence: 0xef11ccd5 [unverified]
    [FCS Status: Unverified]
    [WLAN Flags: .....TC]
v IEEE 802.11 Wireless Management
  v Fixed parameters
    Category code: Radio Measurement (5)
    Action code: Neighbor Report Request (4)
    Dialog token: 1
  v Tagged parameters (9 bytes)
    v Tag: SSID parameter set: "WPA-PSK"
      Tag Number: SSID parameter set (0)
      Tag length: 7
      SSID: "WPA-PSK"
```

Neighbor Report Response

```

v IEEE 802.11 Action, Flags: .....C
  Type/Subtype: Action (0x000d)
  > Frame Control Field: 0xd000
    .000 0000 0011 1100 = Duration: 60 microseconds
  > Receiver address: 0a:c2:08:38:9d:b5 (0a:c2:08:38:9d:b5)
  > Destination address: 0a:c2:08:38:9d:b5 (0a:c2:08:38:9d:b5)
  > Transmitter address: Cisco_75:9d:cf (78:72:5d:75:9d:cf)
  > Source address: Cisco_75:9d:cf (78:72:5d:75:9d:cf)
  > BSS Id: Cisco 75:9d:cf (78:72:5d:75:9d:cf) ← Current AP's BSSID
    .... 0000 = Fragment number: 0
    0010 1111 1101 .... = Sequence number: 765
    Frame check sequence: 0x34931a77 [unverified]
    [FCS Status: Unverified]
    [WLAN Flags: .....C]
v IEEE 802.11 Wireless Management
v Fixed parameters
  Category code: Radio Measurement (5)
  Action code: Neighbor Report Response (5)
  Dialog token: 1
v Tagged parameters (15 bytes)
  v Tag: Neighbor Report
    Tag Number: Neighbor Report (52)
    Tag length: 13
    BSSID: Cisco 89:09:ef (7c:21:0d:89:09:ef) ← Neighbor AP's BSSID
  > BSSID Information: 0x000002f7
    Operating Class: 118
    Channel Number: 64 (iterative measurements on that Channel Number)
    PHY Type: 0x07

```



802.11k Support

- + Not all access points and Wi-Fi clients support 802.11k
- + Access points indicate 802.11k support in the RM Capability Information Element (IE) present in;
 - + Beacons
 - + Probe Responses
- + WLAN clients indicate support in Association and Re-association Request frames

Verifying 802.11k Access Point Support

+ 802.11k “Neighbor List” support advertised in Beacons

```
> 802.11 radio information
> IEEE 802.11 Beacon frame, Flags: .....C
v IEEE 802.11 Wireless Management
  > Fixed parameters (12 bytes)
  v Tagged parameters (290 bytes)
    > Tag: SSID parameter set: "WPA-PSK"
    > Tag: Supported Rates 6(B), 9, 12(B), 18, 24(B), 36, 48, 54, [Mbit/sec]
    > Tag: DS Parameter set: Current Channel: 64
    > Tag: Traffic Indication Map (TIM): DTIM 0 of 1 bitmap
    > Tag: Country Information: Country Code US, Environment All
    > Tag: Power Constraint: 0
    > Tag: QBSS Load Element 802.11e CCA Version
    v Tag: RM Enabled Capabilities (5 octets)
      Tag Number: RM Enabled Capabilities (70)
      Tag length: 5
      v RM Capabilities: 0x73 (octet 1)
        .... ..1 = Link Measurement: Enabled
        .... ..1. = Neighbor Report: Enabled
        .... .0.. = Parallel Measurements: Disabled
        .... 0... = Repeated Measurements: Disabled
        ...1 .... = Beacon Passive Measurement: Enabled
        ..1. .... = Beacon Active Measurement: Enabled
        .1.. .... = Beacon Table Measurement: Supported
        0... .... = Beacon Measurement Reporting Conditions: Disabled
```

Verifying 802.11k WLAN Client Support

- + 802.11k “Neighbor List” support advertised in Association Request Frames

```
109 2.680268 0a:c2:08:38:9d:b5 Cisco_75:9d:cf 802.11 268 Association Request,
> Frame 109: 268 bytes on wire (2144 bits), 268 bytes captured (2144 bits)
> Radiotap Header v0, Length 36
> 802.11 radio information
> IEEE 802.11 Association Request, Flags: .....C
v IEEE 802.11 Wireless Management
  > Fixed parameters (4 bytes)
  v Tagged parameters (200 bytes)
    > Tag: SSID parameter set: "WPA-PSK"
    > Tag: Supported Rates 6(B), 9, 12(B), 18, 24(B), 36, 48, 54, [Mbit/sec]
    > Tag: Operating Mode Notification
    > Tag: Power Capability Min: 8, Max: 20
    > Tag: Supported Channels
    > Tag: HT Capabilities (802.11n D1.10)
    > Tag: RSN Information
    > Tag: Supported Operating Classes
    v Tag: RM Enabled Capabilities (5 octets)
      Tag Number: RM Enabled Capabilities (70)
      Tag length: 5
    v RM Capabilities: 0x73 (octet 1)
      .... ..1 = Link Measurement: Enabled
      .... ..1. = Neighbor Report: Enabled
      .... .0.. = Parallel Measurements: Disabled
      .... 0... = Repeated Measurements: Disabled
      ...1 .... = Beacon Passive Measurement: Enabled
      ..1. .... = Beacon Active Measurement: Enabled
      .1. .... = Beacon Table Measurement: Supported
      0... .... = Beacon Measurement Reporting Conditions: Disabled
```



Cisco Catalyst 9800 Support

- + 802.11k is supported on Cisco Catalyst 9800 WLCs and most Cisco Access Points
- + Can be enabled or disabled per WLAN/SSID in GUI or CLI
- + Found in the WLAN configuration profile, under “Advanced”

Verifying 802.11k in Web-UI

- + New WLANs have 802.11k enabled by default

The screenshot shows the Cisco Web-UI configuration page for WLANs. The breadcrumb navigation is 'Configuration > Tags & Profiles > WLANs'. The 'Add WLAN' button is circled in red. The 'Advanced' tab is selected, showing the following settings:

Setting	Value
Coverage Hole Detection	<input checked="" type="checkbox"/>
Aironet IE	<input type="checkbox"/>
Advertise AP Name	<input type="checkbox"/>
P2P Blocking Action	Disabled
Multicast Buffer	<input type="checkbox"/> DISABLED
Universal Admin	<input type="checkbox"/>
OKC	<input checked="" type="checkbox"/>
Load Balance	<input type="checkbox"/>
Best Select	<input type="checkbox"/>

The 'Assisted Roaming (11k)' section is highlighted with a red box and contains the following settings:

Setting	Value
Prediction Optimization	<input type="checkbox"/>
Neighbor List	<input checked="" type="checkbox"/>
Dual Band Neighbor List	<input type="checkbox"/>

Verifying Neighbor Lists

- + IOS-XE on 9800 provides a command to view 802.11k neighbors per access point.

```
9800-1#show ap name AP7872.5D73.F706 auto-rf dot11 5ghz
#####

Number of Slots                : 2
AP Name                        : AP7872.5D73.F706
MAC Address                    : 7872.5d75.9dc0
Ethernet MAC Address          : 7872.5d73.f706
  Slot ID                      : 1
  Radio Type                   : 802.11ac
  Subband Type                 : All

Noise Information
  Noise Profile                : Passed
  Channel 36                   : -94 dBm
  Channel 40                   : -94 dBm
```

```
Nearby APs
  AP 7c21.0d89.09ef slot 1      : -31 dBm on ( 64, 40 MHz) (10.199.199.254)
```





**Thank you for
watching!!**



802.11v: It's Time to Move On

<https://t.me/learningnets>



The Problem 802.11v Was Designed to Solve

- + Wi-Fi clients often "stick" to a weak AP far longer than optimal
- + Legacy roaming is entirely client-driven with no input from the network
- + This leads to:
 - + Poor performance (low RSSI, low throughput, high retries)
 - + Congestion on overloaded APs
 - + Suboptimal roaming decisions
- + Network administrators needed a standardized way *to guide or influence roaming behavior*

What is IEEE 802.11v?

- + A Wi-Fi standard amendment focused on Wireless Network Management (WNM)
- + Adds the ability for the AP/network to suggest better APs to clients
- + Most important feature → BSS Transition Management
- + Goal: Assist roaming decisions based on network knowledge and policy

802.11v Key Functional Behavior

- + AP-initiated or client-initiated roaming suggestions:
 - + AP sends a *BSS Transition Management Request*
 - + Client may send a *BSS Transition Management Query* (solicited request)
- + Candidate list of AP's with the current AP's "Request" includes:
 - + BSSID, Channel, Preference value
- + Client responds with:
 - + *BSS Transition Management Response* (accept, reject, or defer)
- + Roaming still remains client-controlled

Contrasting .11k to .11v

Feature	802.11k	802.11v
Who initiates?	Client	AP (or client as a query)
What is exchanged?	Neighbor list	Roaming recommendations
Data format?	Neighbor Report	BSS Transition Management Frames
Timing?	Preemptive scan optimization	Reactive or policy-driven nudges
Purpose?	Faster scanning	Load balancing / coverage fixes

Verifying 802.11v Access Point Support

+ 802.11v “BSS Transition” support advertised in Beacons

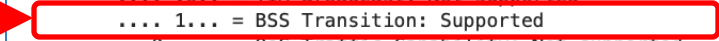
```
2196 60.407629 Cisco_75:9d:cf Broadcast 802.11 358 Beacon frame,
-----
  Tagged parameters (282 bytes)
    > Tag: SSID parameter set: "WPA-PSK"
    > Tag: Supported Rates 6(B), 9, 12(B), 18, 24(B), 36, 48, 54, [Mbit/sec]
    > Tag: DS Parameter set: Current Channel: 100
    > Tag: Traffic Indication Map (TIM): DTIM 0 of 1 bitmap
    > Tag: Country Information: Country Code US, Environment All
    > Tag: Power Constraint: 0
    > Tag: RSN Information
    > Tag: QBSS Load Element 802.11e CCA Version
    > Tag: HT Capabilities (802.11n D1.10)
    > Tag: HT Information (802.11n D1.10)
  < Tag: Extended Capabilities (8 octets)
    Tag Number: Extended Capabilities (127)
    Tag length: 8
    > Extended Capabilities: 0x00 (octet 1)
    > Extended Capabilities: 0x00 (octet 2)
  < Extended Capabilities: 0x08 (octet 3)
    .... 0 = TFS: Not supported
    .... 0. = WNM Sleep Mode: Not supported
    .... 0.. = TIM Broadcast: Not supported
    .... 1... = BSS Transition: Supported
    .... 0... = QoS Traffic Capability: Not supported
    ..0. .... = AC Station Count: Not supported
    .0.. .... = https://1me/learnings supported
    0... .... = Timing Measurement: Not supported
```



Verifying 802.11v WLAN Client Support

- + 802.11v “BSS Transition” support advertised in Association Request Frames

```
0a:c2:08:38:9d:b5 Cisco_75:9d:cf 802.11 268 Association Request,
IEEE 802.11 Wireless Management
  Fixed parameters (4 bytes)
    Capabilities Information: 0x1111
    Listen Interval: 0x0001
  Tagged parameters (200 bytes)
    Tag: SSID parameter set: "WPA-PSK"
      Tag Number: SSID parameter set (0)
      Tag length: 7
      SSID: "WPA-PSK"
    Tag: Supported Rates 6(B), 9, 12(B), 18, 24(B), 36, 48, 54, [Mbit/sec]
    Tag: Operating Mode Notification
    Tag: Power Capability Min: 8, Max: 20
    Tag: Supported Channels
    Tag: HT Capabilities (802.11n D1.10)
    Tag: RSN Information
    Tag: Supported Operating Classes
    Tag: RM Enabled Capabilities (5 octets)
    Tag: Extended Capabilities (8 octets)
      Tag Number: Extended Capabilities (127)
      Tag length: 8
      Extended Capabilities: 0x00 (octet 1)
      Extended Capabilities: 0x00 (octet 2)
      Extended Capabilities: 0x08 (octet 3)
        ... 0 = TFS: Not supported
        ... 0 = WMM Sleep Mode: Not supported
        ... 0 = TIM Broadcast: Not supported
        ... 1... = BSS Transition: Supported
        ... 0 ... = QoS Traffic Capability: Not supported
        ... 0 ... = AC Station Count: Not supported
        ... 0 ... = HT Protection: Not supported
        ... 0 ... = Timing Measurement: Not supported
```



Enabling 802.11v on Catalyst 9800s

- + 802.11v BSS-Transition enabled by default

The screenshot shows the 'Edit WLAN' configuration page for a Catalyst 9800. The 'Advanced' tab is selected and circled in red. A red dashed arrow points from the '11v BSS Transition Support' section to the 'BSS Transition' checkbox, which is checked. Other settings include 'Dual Neighbor List' (checked), 'BSS Max Idle Service' (unchecked), 'BSS Max Idle Protected' (unchecked), and 'Directed Multicast Service' (unchecked). On the right side, 'Universal Admin' (unchecked), 'OKC' (unchecked), 'Load Balance' (unchecked), 'Band Select' (unchecked), 'IP Source Guard' (unchecked), 'WMM Policy' (Allowed), and 'mDNS Mode' (Bridging) are visible. A warning message at the top states: 'Changing WLAN parameters while it is enabled will result in loss of connectivity for clients connected to it.'

11v BSS Transition Support

BSS Transition	<input checked="" type="checkbox"/>
Dual Neighbor List	<input checked="" type="checkbox"/>
BSS Max Idle Service	<input type="checkbox"/>
BSS Max Idle Protected	<input type="checkbox"/>
Directed Multicast Service	<input type="checkbox"/>

<https://t.me/learningnets>



**Thank you for
watching!!**



The Robust Security Network

<https://t.me/learningnets>



Key Steps in Client Roaming

- + To comprehend the roaming process and what part(s) of it could cause unacceptable delays one needs to understand;
 - + The frame exchanges used in roaming
 - + The purpose of those frame exchanges
- + The overall process of roaming involves the following;
 - + Client's introduction to the new access point
 - + *Authentication of the client*
 - + *Derivation and distribution of encryption keys for that client's session.*
- + The last two items above are covered by RSN

Robust Security Network

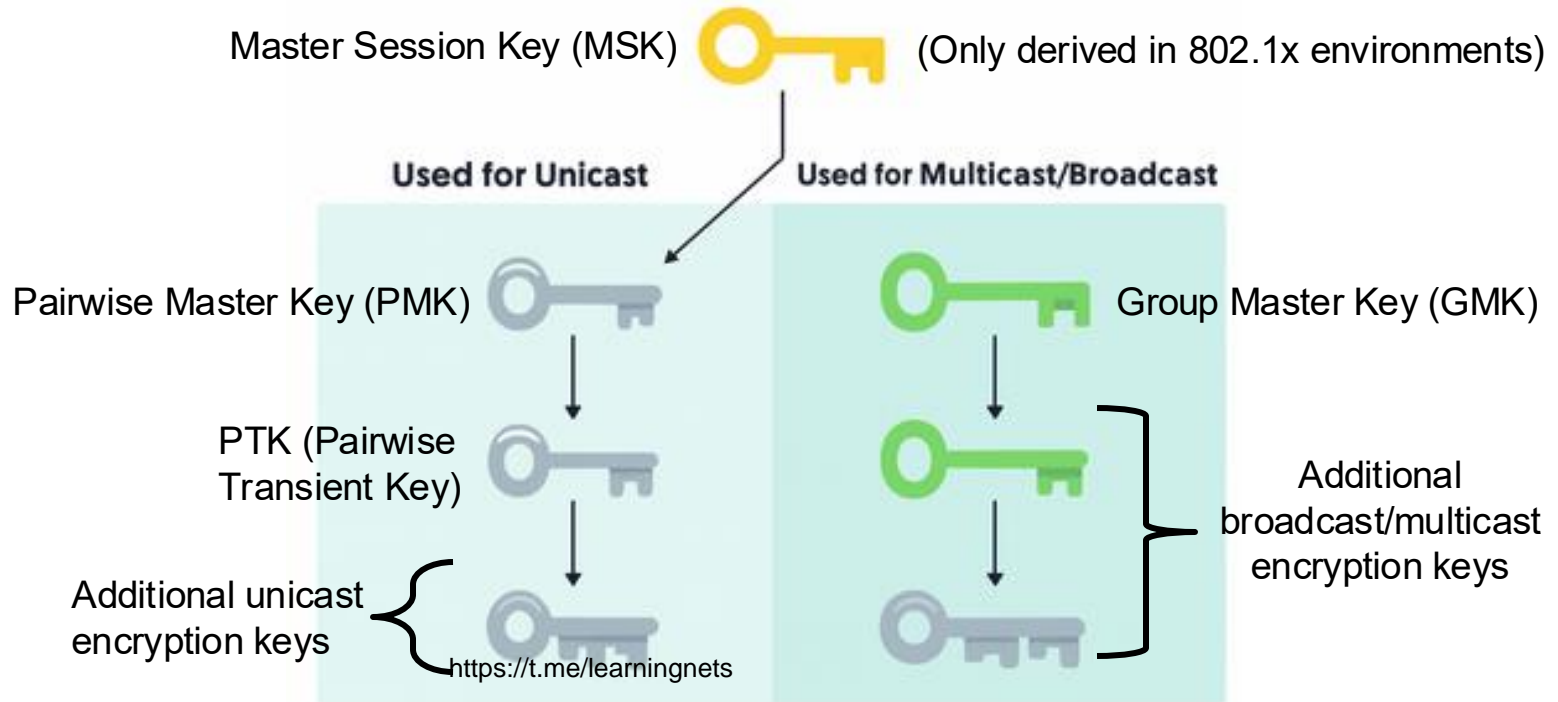
- + RSN was introduced in 802.11i
 - + *RSN = Wireless networks that leverage cryptography to provide data integrity and confidentiality between WLAN client and AP*
 - + Utilizes a hierarchy of cryptographic keys generated, and used during a wireless session
- + Certified by WPA2 or WPA3 to manage key generation and other security mechanisms
 - + WPA was pre-802.11i

RSN Goals

- + There are several goals of RSN some of which can negatively affect roaming;
 - + Authentication-induced latency
 - + Encryption key-derivation and sharing latency
- + WPA-2/WPA-3 Enterprise requires the use of 802.1x and Radius exchanges with an authentication server
 - + *Keys are generated after authentication*
- + Radius and 802.1x not used with;
 - + WPA2 Personal (PSK)
 - + WPA3 Personal (SAE)

Overview of RSN Keys

- + Once authentication has been completed, RSN dictates the generation and distribution of several types of keys



How to View RSN Information

- + RSN capability information elements (IE's) are visible within various 802.11 management frames.

Source	Destination	Protocol	Length	Info
Cisco_75:9d:cf	Broadcast	802.11	358	Beacon frame, SN=1983, FN=0, Flags=.

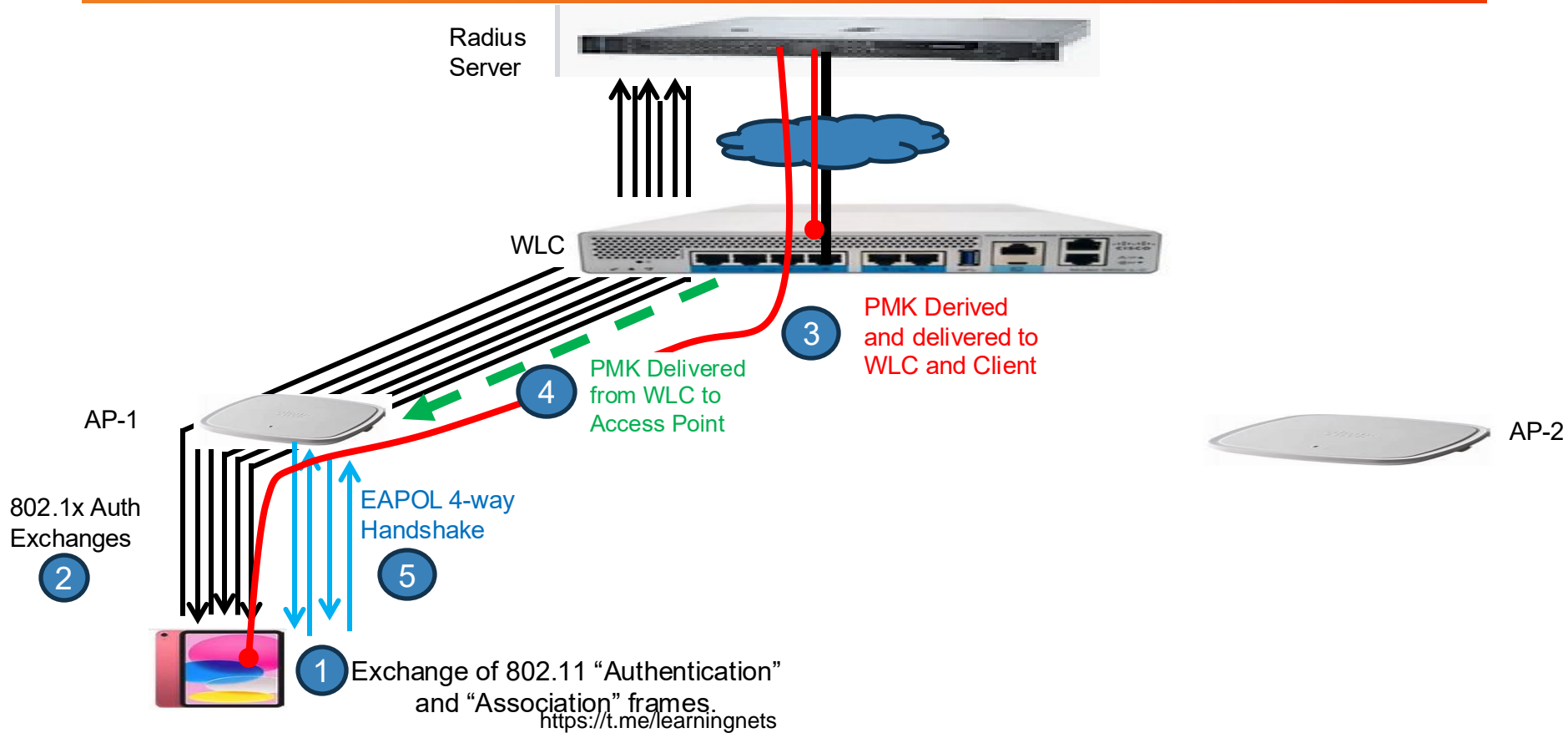

```
> Frame 1: 358 bytes on wire (2864 bits), 358 bytes captured (2864 bits)
> Radiotap Header v0, Length 36
> 802.11 radio information
> IEEE 802.11 Beacon frame, Flags: .....C
< IEEE 802.11 Wireless Management
  > Fixed parameters (12 bytes)
  < Tagged parameters (282 bytes)
    > Tag: SSID parameter set: "WPA-PSK"
    > Tag: Supported Rates 6(B), 9, 12(B), 18, 24(B), 36, 48, 54, [Mbit/sec]
    > Tag: DS Parameter set: Current Channel: 100
    > Tag: Traffic Indication Map (TIM): DTIM 0 of 1 bitmap
    > Tag: Country Information: Country Code US, Environment All
    > Tag: Power Constraint: 0
    < 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) PSK
    > RSN Capabilities: https://www.learningnets
```

WPA2 / WPA3 Enterprise Association

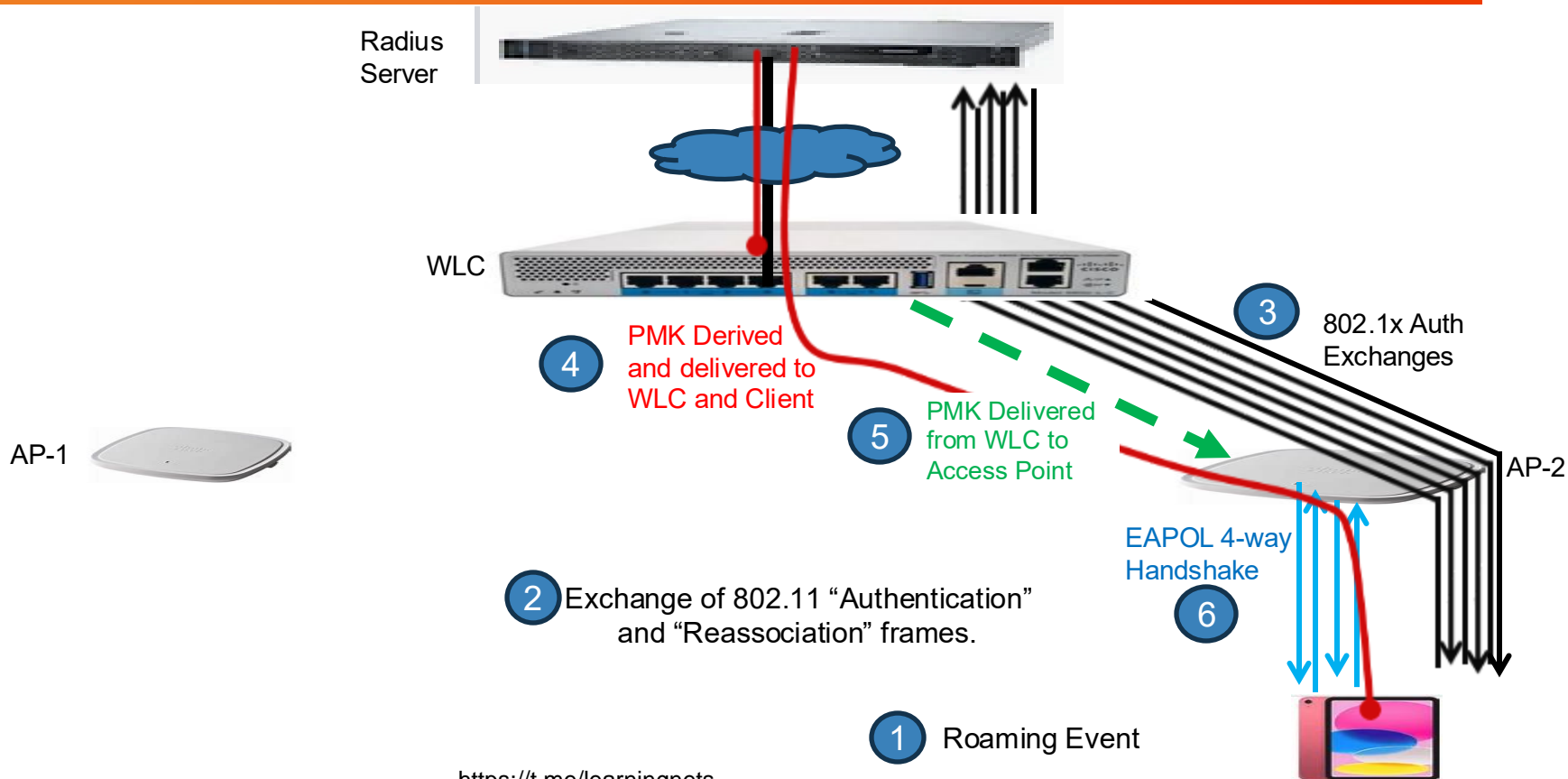
1. 802.11 Authentication and Association messages are exchanged between the AP (or WLC) and the client
2. 802.1x EAP authentication occurs
 - a. Client provides security credentials
 - b. AP then authenticates against a RADIUS server
 - c. This exchange is typically 8-14 messages long
 - d. Both the AP and the client receive a master-key known as the PMK
3. EAPOL 4-way handshake in which encryption keys are derived from the per-session PMK (used for encrypting all traffic between the AP and the client).

This is where extreme delay can occur

WPA-Enterprise RSN Association Process



WPA-Enterprise RSN Reassociation Process



What About WPA-2/WPA-3 Personal?

- + WPA-2 / WPA-3 Personal also requires derivation of keys
 - + PMK
 - + PTK
 - + Etc
- + EAPOL 4-way handshake still required
- + Mechanism for derivation of material used before EAPOL handshake differs than WPA Enterprise

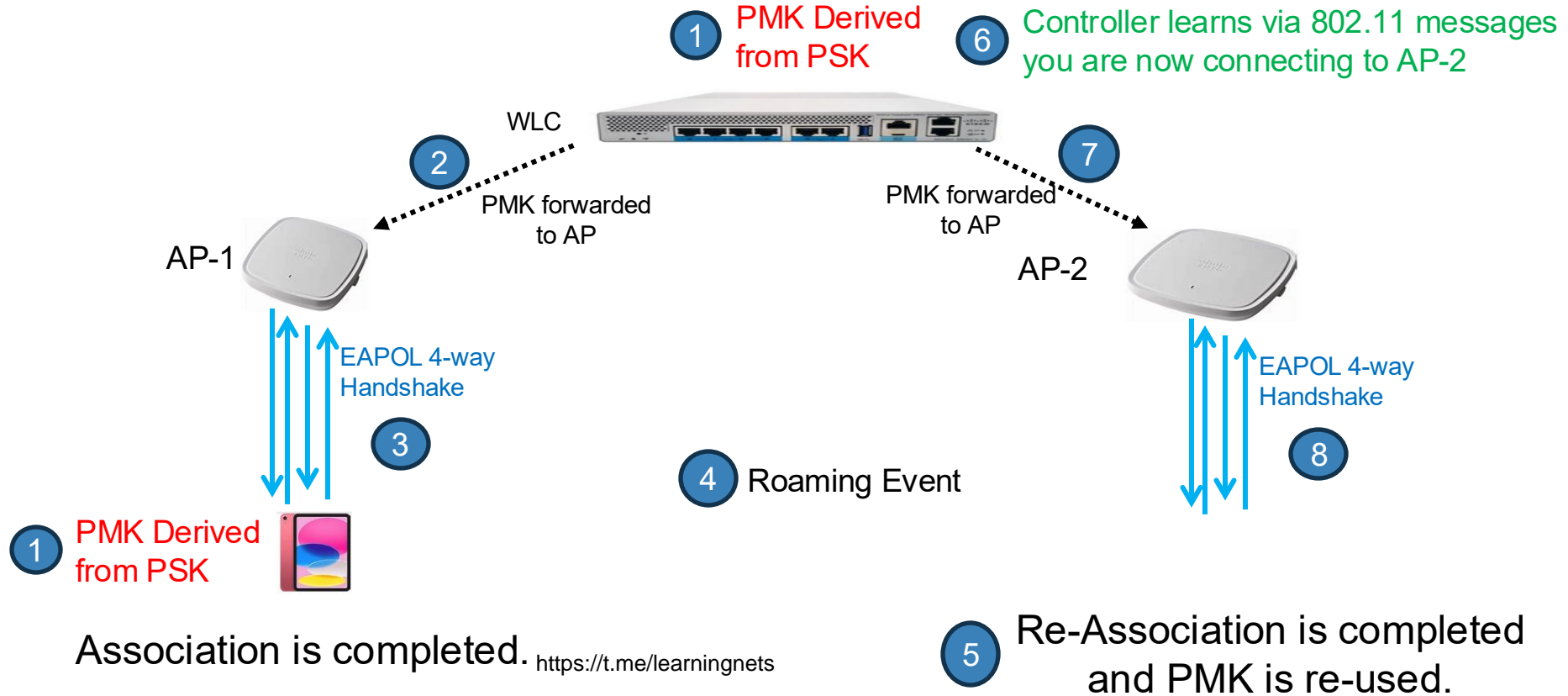
WPA PSK Handshake

304	2.091412	86:6c:b8:16:5e:89	TpLinkTechno_81:3...	802.11	157	Probe Request, SN=2075, FN=0, Flags=.....C, SSID="SkippyPip"
306	2.092083	TpLinkTechno_81:32:...	86:6c:b8:16:5e:89	802.11	468	Probe Response, SN=2990, FN=0, Flags=.....C, BI=100, SSID="SkippyPip"
308	2.092153	86:6c:b8:16:5e:89	TpLinkTechno_81:3...	802.11	70	Authentication, SN=2076, FN=0, Flags=.....C
310	2.093285	TpLinkTechno_81:32:...	86:6c:b8:16:5e:89	802.11	70	Authentication, SN=2091, FN=0, Flags=.....C
314	2.105668	86:6c:b8:16:5e:89	TpLinkTechno_81:3...	802.11	272	Association Request, SN=2077, FN=0, Flags=.....C, SSID="SkippyPip"
316	2.107910	TpLinkTechno_81:32:...	86:6c:b8:16:5e:89	802.11	248	Association Response, SN=2992, FN=0, Flags=.....C
320	2.119001	TpLinkTechno_81:32:...	86:6c:b8:16:5e:89	EAPOL	171	Key (Message 1 of 4)
330	2.136995	86:6c:b8:16:5e:89	TpLinkTechno_81:3...	EAPOL	193	Key (Message 2 of 4)
332	2.147976	TpLinkTechno_81:32:...	86:6c:b8:16:5e:89	EAPOL	275	Key (Message 3 of 4)
334	2.149832	86:6c:b8:16:5e:89	TpLinkTechno_81:3...	EAPOL	171	Key (Message 4 of 4)

```
> Tag: RM Enabled Capabilities (5 octets)
> Tag: HT Capabilities (802.11n D1.10)
> Tag: HT Information (802.11n D1.10)
> Tag: Overlapping BSS Scan Parameters
> Tag: Extended Capabilities (8 octets)
> Tag: VHT Capabilities
> Tag: VHT Operation
> Tag: Tx Power Envelope
> Tag: Vendor Specific: Microsoft Corp.: WMM/WME: Parameter Element
> Tag: Vendor Specific: Atheros Communications, Inc.: Advanced Capability
> Tag: Vendor Specific: Qualcomm Inc.
> Tag: Vendor Specific: Microsoft Corp.: WPA Information Element
< Tag: RSN Information
  Tag Number: RSN Information (48)
  Tag length: 24
  RSN Version: 1
  > Group Cipher Suite: 00:0f:ac (Ieee 802.11) TKIP
    Pairwise Cipher Suite Count: 2
  > Pairwise Cipher Suite List 00:0f:ac (Ieee 802.11) AES (CCM) 00:0f:ac (Ieee 802.11) TKIP
    Auth Key Management (AKM) Suite Count: 1
  < Auth Key Management (AKM) List 00:0f:ac (Ieee 802.11) PSK
    < Auth Key Management (AKM) Suite: 00:0f:ac (Ieee 802.11) PSK
      Auth Key Management (AKM) OUI: 00:0f:ac (Ieee 802.11)
      Auth Key Management (AKM) type: PSK (2)
```

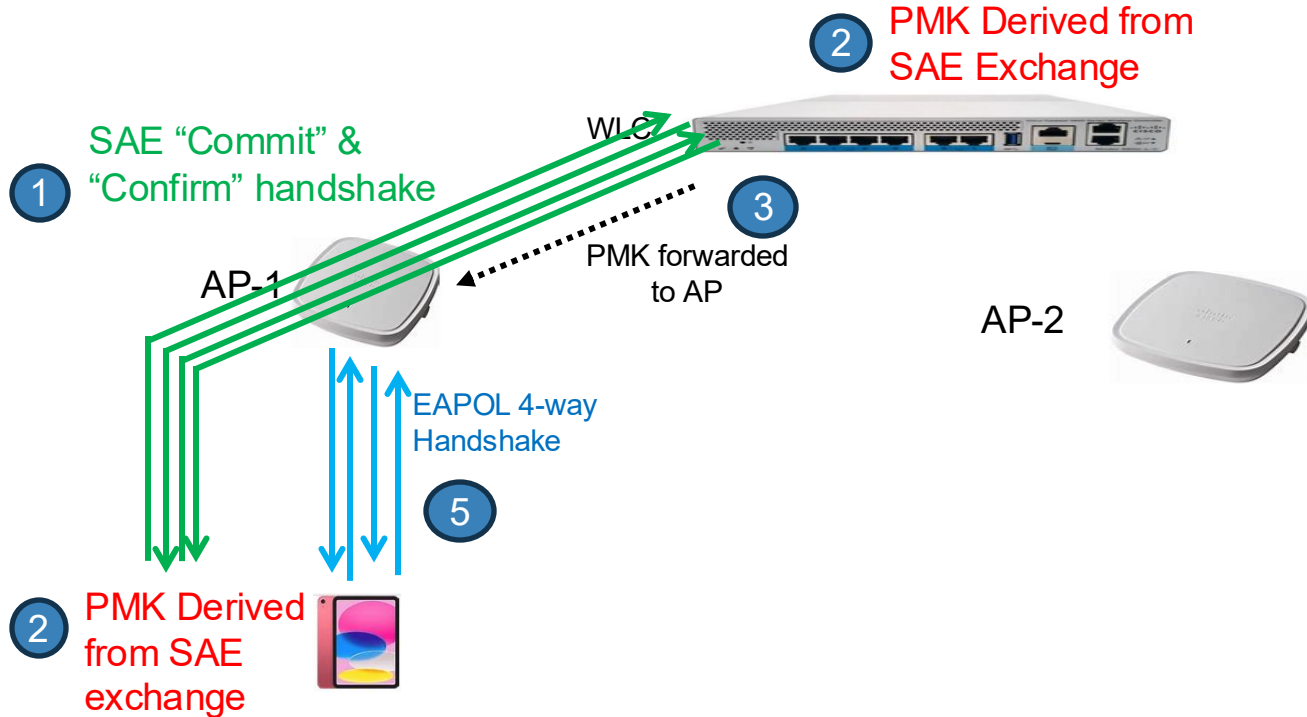
```
0010 12 0c 99 16 40 01 e7 a5 00 02 00 10 18 03 04 00
0020 02 00 00 00 50 00 3c 00 86 6c b8 16 5e 89 50 d4
0030 f7 81 32 d8 50 d4 f7 81 32 d8 e0 ba 51 e4 10 64
0040 2b 02 00 00 64 00 11 15 00 09 53 6b 69 70 70 79
0050 50 69 70 01 08 8c 12 98 24 b0 48 60 6c 03 01 9d
0060 46 05 73 d0 00 00 0c 2d 1a ef 09 03 ff ff ff 00
0070 00 00 00 00 00 00 00 00 01 00 00 00 00 00 00
0080 00 00 00 3d 16 9d 05 04 00 00 00 00 00 00 00
0090 00 00 00 00 00 00 00 00 00 00 00 4a 0e 14 00 0a
00a0 00 2c 01 c8 00 14 00 05 00 19 00 7f 08 05 00 0f
00b0 02 00 00 00 40 bf 0c f2 79 82 33 ea ff 00 00 ea
00c0 ff 00 20 c0 05 01 9b 00 fc ff c3 05 03 3c 3c 3c
00d0 3c dd 18 00 50 f2 02 01 01 80 00 03 a4 00 00 27
00e0 a4 00 00 42 43 5e 00 62 32 2f 00 dd 09 00 43 7f
00f0 01 01 00 00 ff 7f dd 16 8c fd f0 04 00 00 09 4c
0100 51 03 02 09 72 01 8c 16 00 00 46 00 00 00 dd 1a
0110 00 50 f2 01 01 00 00 50 f2 02 02 00 00 50 f2 04
0120 00 50 f2 02 01 00 00 50 f2 02 30 18 01 00 00 0f
0130 ac 02 02 00 00 0f ac 04 00 0f ac 02 01 00 00 0f
0140 ac 02 00 00 dd 80 00 50 f2 04 10 4a 00 01 10 10
0150 44 00 01 02 10 3b 00 01 03 10 47 00 10 87 65 43
0160 21 9a bc de f0 12 34 50 d4 f7 81 32 d9 10 21 00
0170 07 54 50 2d 4c 69 6e 6b 10 23 00 09 41 72 63 68
0180 65 72 5f 41 39 10 24 00 03 31 2e 30 10 42 00 0c
0190 41 72 63 68 65 72 20 41 39 20 76 36 10 54 00 08
01a0 00 06 00 50 f2 04 00 01 10 11 00 0a 41 72 63 68
01b0 65 72 41 39 76 36 10 00 00 02 00 0a 41 72 63 68
```

WPA-2 Personal Roaming RSN Process



Association is completed. <https://t.me/learningnets>

WPA-3 Personal Roaming RSN Process



1 802.11 Authentication contains SAE exchanges

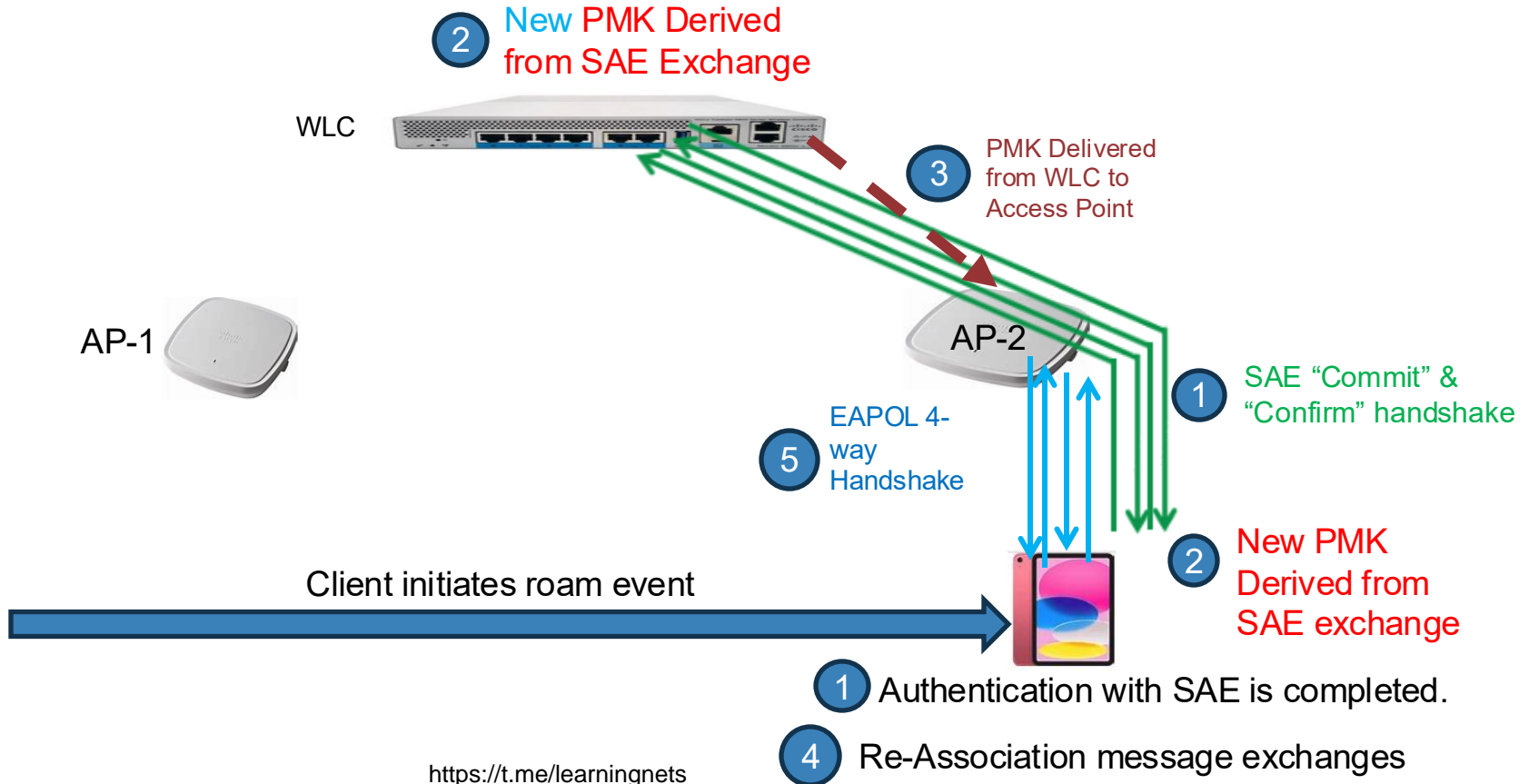
4 802.11 Association Message exchange. <https://t.me/learningnets>

WPA3 SAE Exchanges

Source	Destination	Protocol	Length	Info
fe:e0:cb:b6:76:2f	Cisco_75:9d:cf	802.11	168	Authentication, SN=2417, FN=0, Flags=.....C
Cisco_75:9d:cf	fe:e0:cb:b6:76:2f	802.11	168	Authentication, SN=2986, FN=0, Flags=.....C
fe:e0:cb:b6:76:2f	Cisco_75:9d:cf	802.11	104	Authentication, SN=2418, FN=0, Flags=.....C
Cisco_75:9d:cf	fe:e0:cb:b6:76:2f	802.11	104	Authentication, SN=2987, FN=0, Flags=.....C
fe:e0:cb:b6:76:2f	Cisco_75:9d:cf	802.11	283	Association Request, SN=2419, FN=0, Flags=.....C, SSID="WPA-PSK"
Cisco_75:9d:cf	fe:e0:cb:b6:76:2f	802.11	199	Association Response, SN=2988, FN=0, Flags=.....C
Cisco_75:9d:cf	fe:e0:cb:b6:76:2f	EAPOL	193	Key (Message 1 of 4)
fe:e0:cb:b6:76:2f	Cisco_75:9d:cf	EAPOL	202	Key (Message 2 of 4)
Cisco_75:9d:cf	fe:e0:cb:b6:76:2f	EAPOL	267	Key (Message 3 of 4)
Cisco_75:9d:cf	fe:e0:cb:b6:76:2f	EAPOL	267	Key (Message 3 of 4)
fe:e0:cb:b6:76:2f	Cisco_75:9d:cf	EAPOL	171	Key (Message 4 of 4)

<ul style="list-style-type: none"> > Frame 303: 168 bytes on wire (1344 bits), 168 bytes captured (1344 bits) > Radiotap Header v0, Length 36 > 802.11 radio information > IEEE 802.11 Authentication, Flags:C <ul style="list-style-type: none"> > IEEE 802.11 Wireless Management <ul style="list-style-type: none"> > Fixed parameters (104 bytes) <ul style="list-style-type: none"> Authentication Algorithm: Simultaneous Authentication of Equals (SAE) (3) Authentication SEQ: 0x0001 Status code: SAE authentication uses direct hashing, instead of looping, to obtain the PWE (0) SAE Message Type: Commit (1) Group Id: 256-bit random ECP group (19) Scalar: 69a842fa48b25872623a5661eefcf787cb5b0c181bc7336ea07540759f45d0a7 Finite Field Element: ca5b78743db725da4bafbfc4486c37cfde2c7a7a22126b917457eb95fef5c889c3eea6b 	<pre> 0000 00 00 24 00 6f 08 00 0010 12 0c cc 15 40 01 e1 0020 02 00 00 00 b0 00 3c 0030 cb b6 76 2f 78 72 5d 0040 7e 00 13 00 69 a8 42 0050 ee fc f7 87 cb 5b 0c 0060 9f 45 d0 a7 ca 5b 78 0070 48 6c 37 cf de 2c 7a 0080 fe f5 c8 89 c3 ee a6 0090 e4 a0 2f 87 7a 7f e3 00a0 67 55 37 80 1b 55 b0 </pre>
--	--

WPA-3 Personal Roaming RSN Process



How Can We Optimize Roaming?

- + RF factors and channel utilization are difficult to optimize via Wi-Fi roaming features
 - + 802.11v can steer clients off a crowded/overloaded AP as part of load-balancing policies
- + The following authentication-induced latency factors can be minimized (or even eliminated completely) depending on the roaming feature selected:
 - + 802.1x/Radius exchange latency with Radius server
 - + SAE Commit/Confirm handshake latency
 - + EAPOL 4-way handshake



**Thank you for
watching!!**

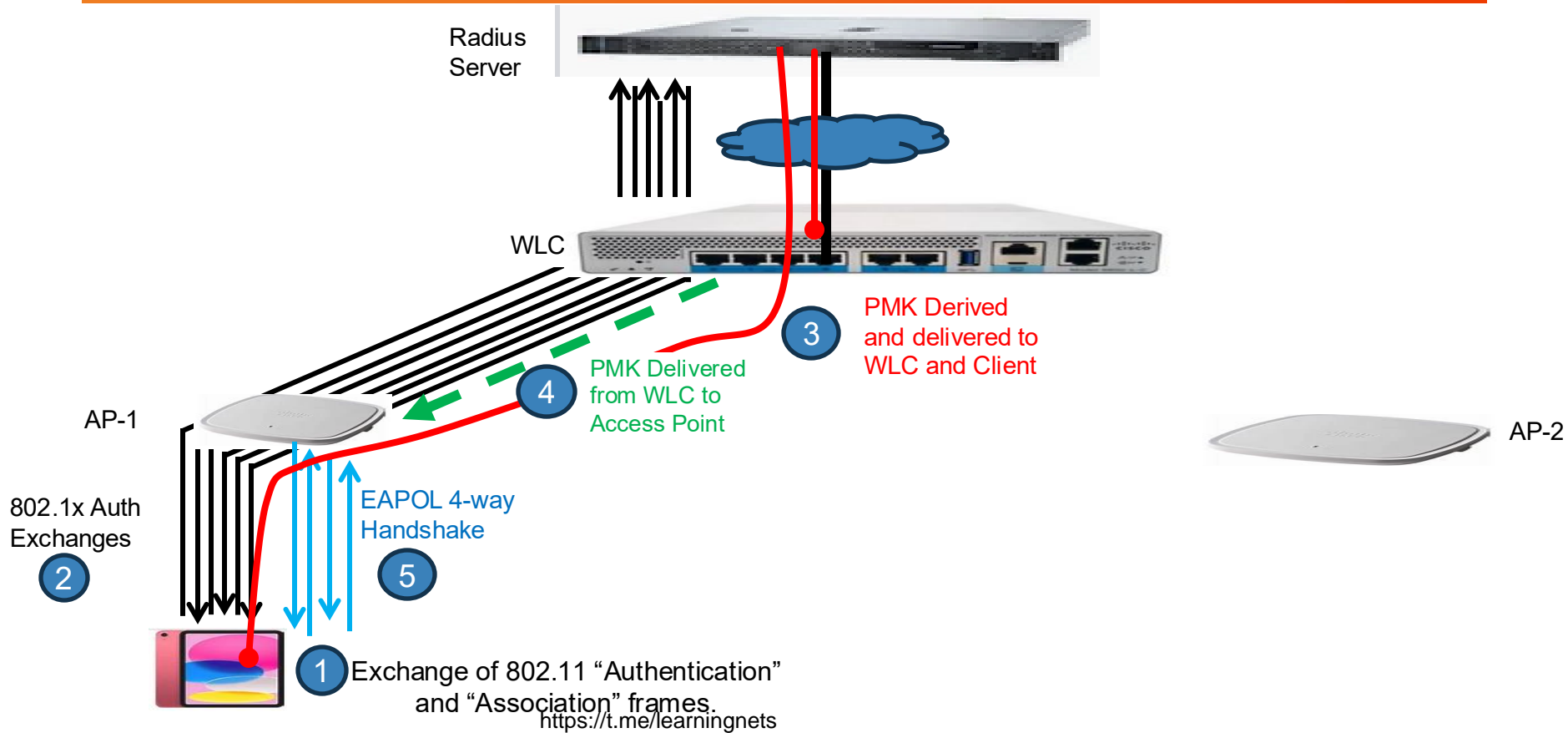


Cisco Centralized Key Management (CCKM)

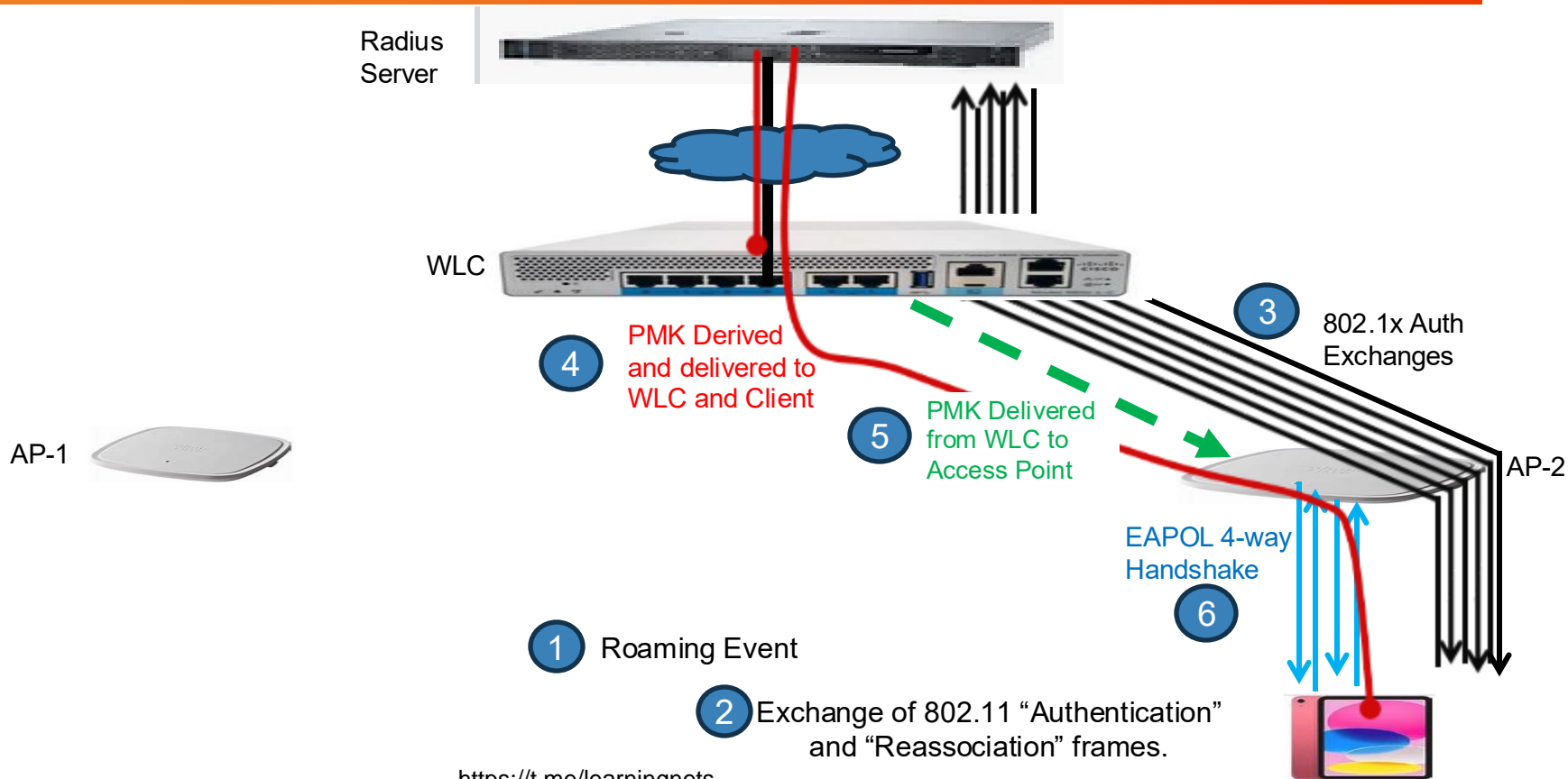
CCKM Overview

- + Cisco Centralized Key Management
 - + Historically, one of the first roaming optimization features developed (2007)
 - + Cisco proprietary
- + Required WLAN client device to run CCX (Cisco Compatible Extensions)
- + Only optimized Enterprise WLAN roams (802.1x)
 - + *Does not optimize or affect WPA-Personal WLAN roaming*

WPA-Enterprise RSN Association Process



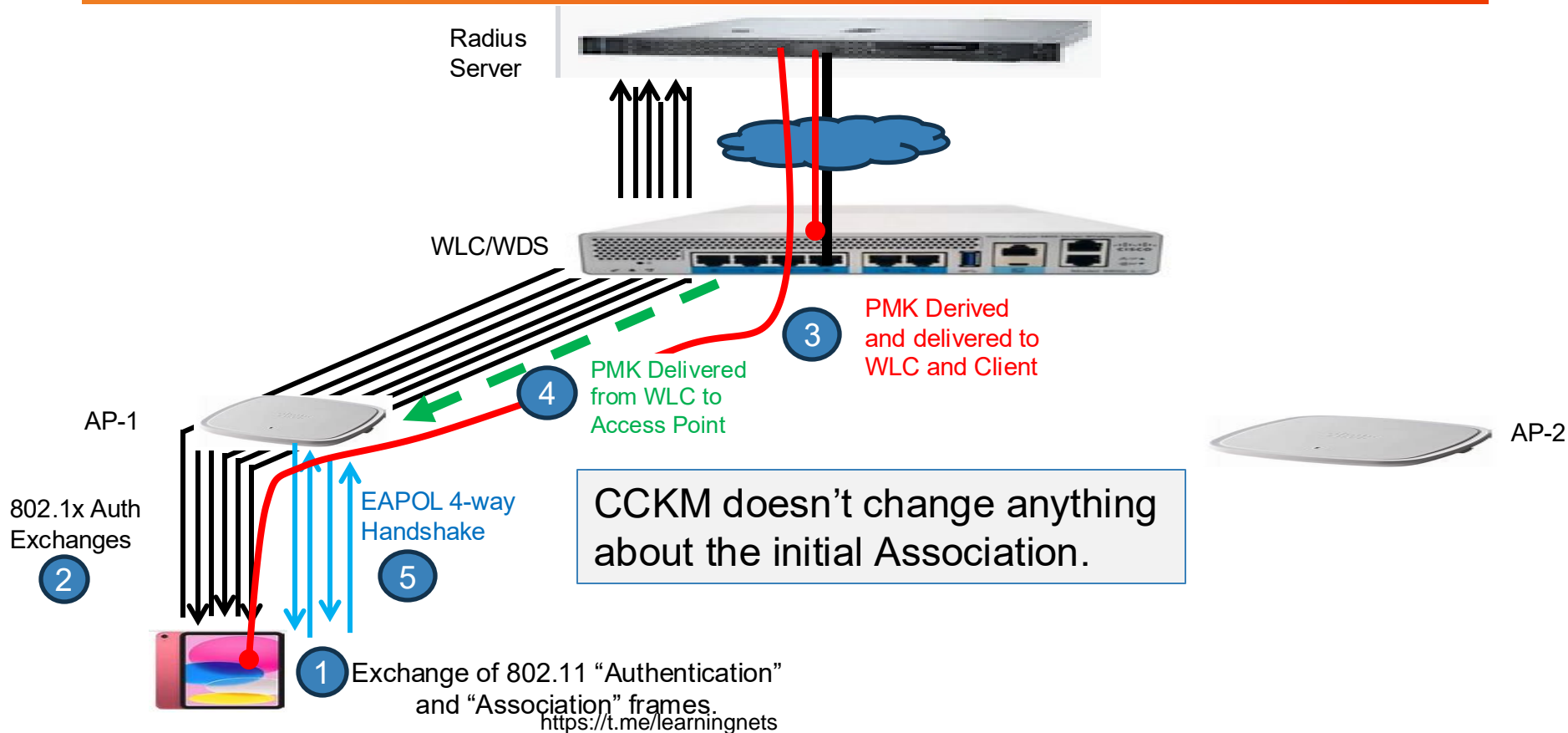
WPA-Enterprise RSN Reassociation Process



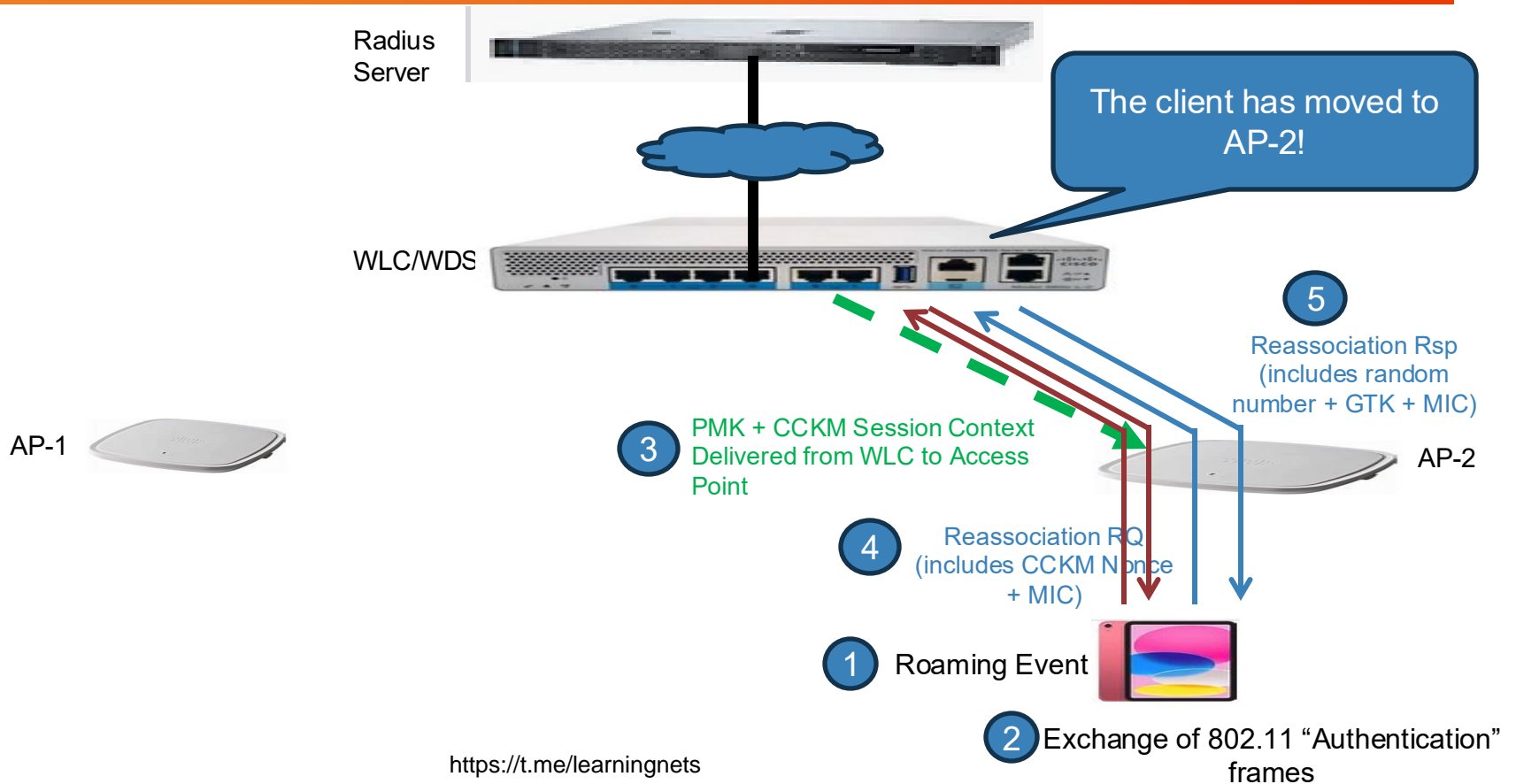
CCKM Operation

- + CCKM relied on a device performing the role of WDS
 - + *Wireless Domain Services*
 - + Could be an autonomous AP, Cisco Router, or Wireless Module within a switch
 - + Now supported by Cisco Catalyst 9800 WLCs (as the WDS)
- + After initial 802.1x authentication, WDS caches client's PMK
- + Clients compatible with CCKM transmit keying material in their Reassociation Request frames.
- + WDS forwards key material and PMK to new access points
- + *Upon a roam, CCKM allows clients to;*
 - + *Skip full 802.1x authentication*
 - + *Skip 4-way EAPOL handshake*

WPA-Enterprise CCKM Association Process



Optimized Roaming with CCKM



Enabling CCKM

- + Most modern Wi-Fi clients no longer support CCKM but, in case you really WANT to enable it...

Edit WLAN

General **Security** Advanced Add To Policy Tags

Layer2 Layer3 AAA

WPA + WPA2 WPA2 + WPA3 WPA3 Static WEP None

MAC Filtering

Fast Transition

Status Disabled

Over the DS

Reassociation Timeout * 20

WPA2 Encryption

AES(CCMP128) CCMP256

GCMP128 GCMP256

Protected Management Frame

PMF Disabled

Auth Key Mgmt

802.1X	<input checked="" type="checkbox"/>	FT	<input type="checkbox"/>
Easy-PSK	<input type="checkbox"/>	CCKM	<input checked="" type="checkbox"/>
FT + 802.1X	<input type="checkbox"/>	FT + PSK	<input type="checkbox"/>
802.1X-SHA256	<input type="checkbox"/>	PSK-SHA256	<input type="checkbox"/>

<https://t.me/learningnets>

CCKM authentication key management will be deprecated soon. Refer to release notes and documentation for more details and migration options.

CCKM ⚠️





**Thank you for
watching!!**



Opportunistic Key Caching (OKC)

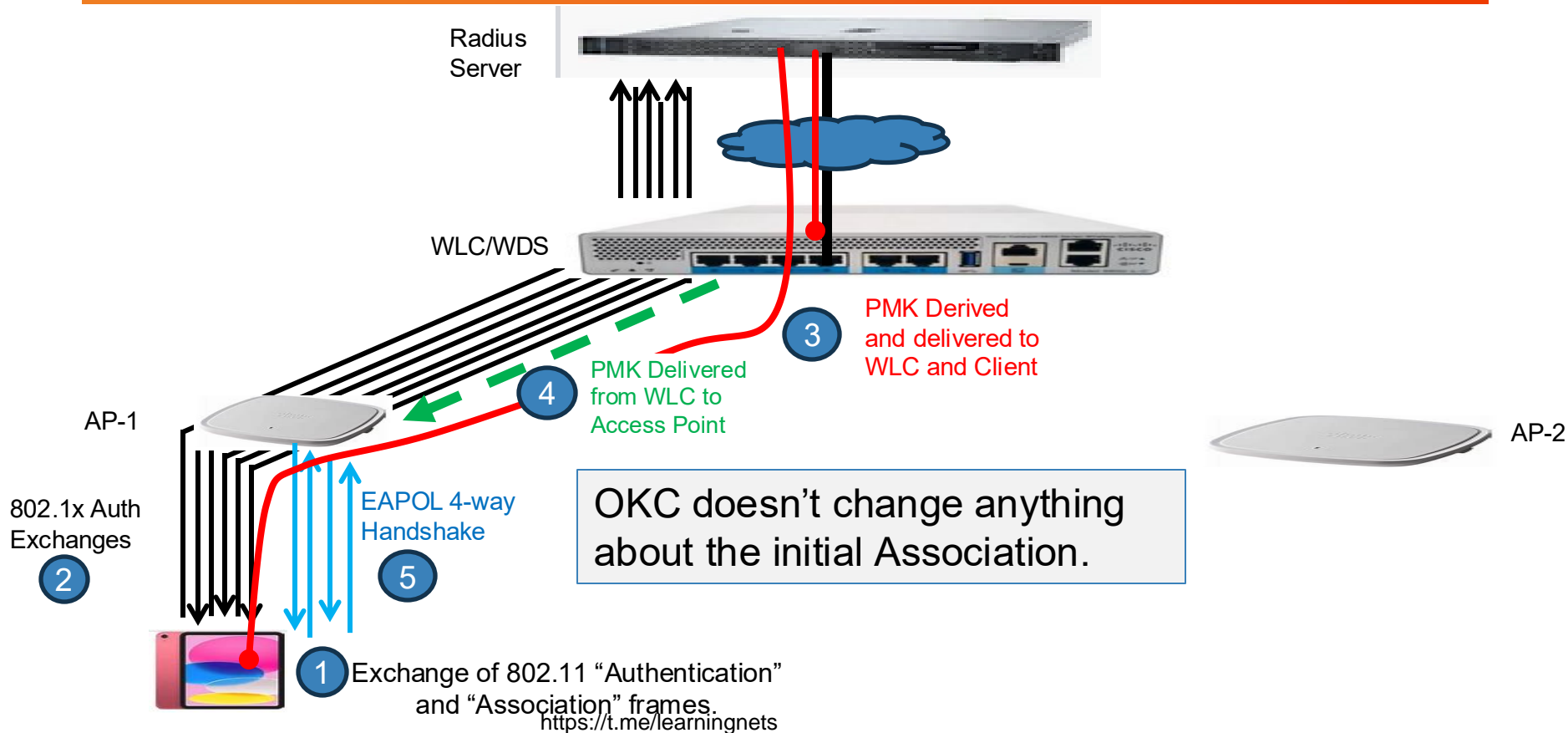
OKC Overview

- + Developed in the mid-2000s, first documented by Microsoft for fast roaming in WPA-Enterprise networks.
- + Adopted by major enterprise Wi-Fi vendors (Cisco, Aruba, Ruckus, etc.) for compatibility with Microsoft clients.
- + Not an IEEE standard — roaming key distribution methods are vendor-specific.
- + *Works by sharing cached Pairwise Master Keys (PMKs) among APs in the same mobility domain.*
- + Primarily benefits WPA-Enterprise; *offers no roaming advantage for WPA-Personal networks.*

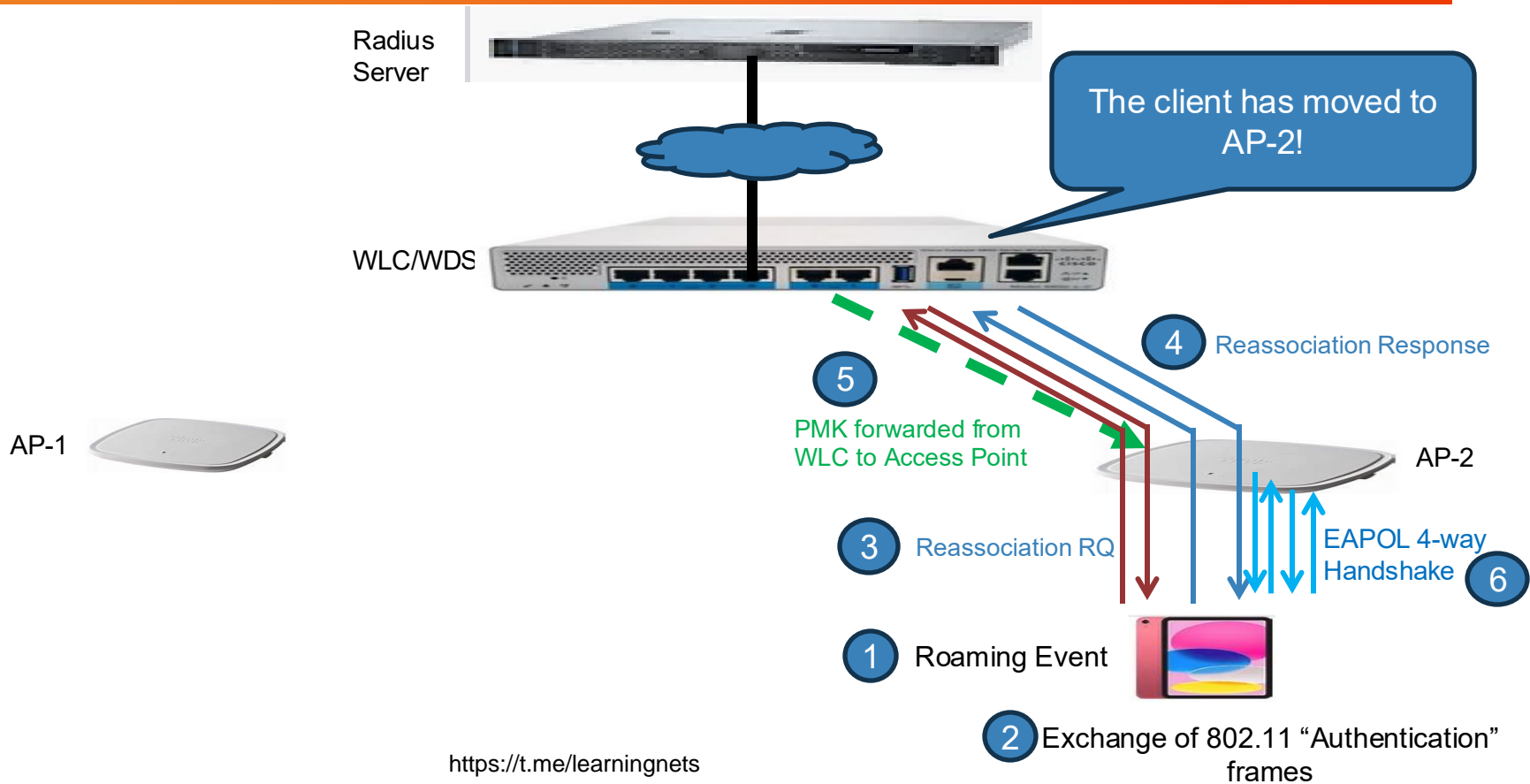
How OKC Works

1. Client detects need to roam → decides on a new AP.
2. Client sends Reassociation Request to the target AP.
3. Target AP forwards the request to the WLC.
4. WLC checks its PMK cache (keyed by client MAC + SSID) to see if a valid PMK exists from a previous 802.1X authentication.
5. If PMK exists:
 - a. WLC sends the PMK to the new AP over the CAPWAP control channel.
 - b. The AP and client then perform the 4-way EAPOL handshake to derive the PTK.
6. If PMK does not exist a full 802.1X/EAP authentication is triggered.

WPA-Enterprise OKC Association Process

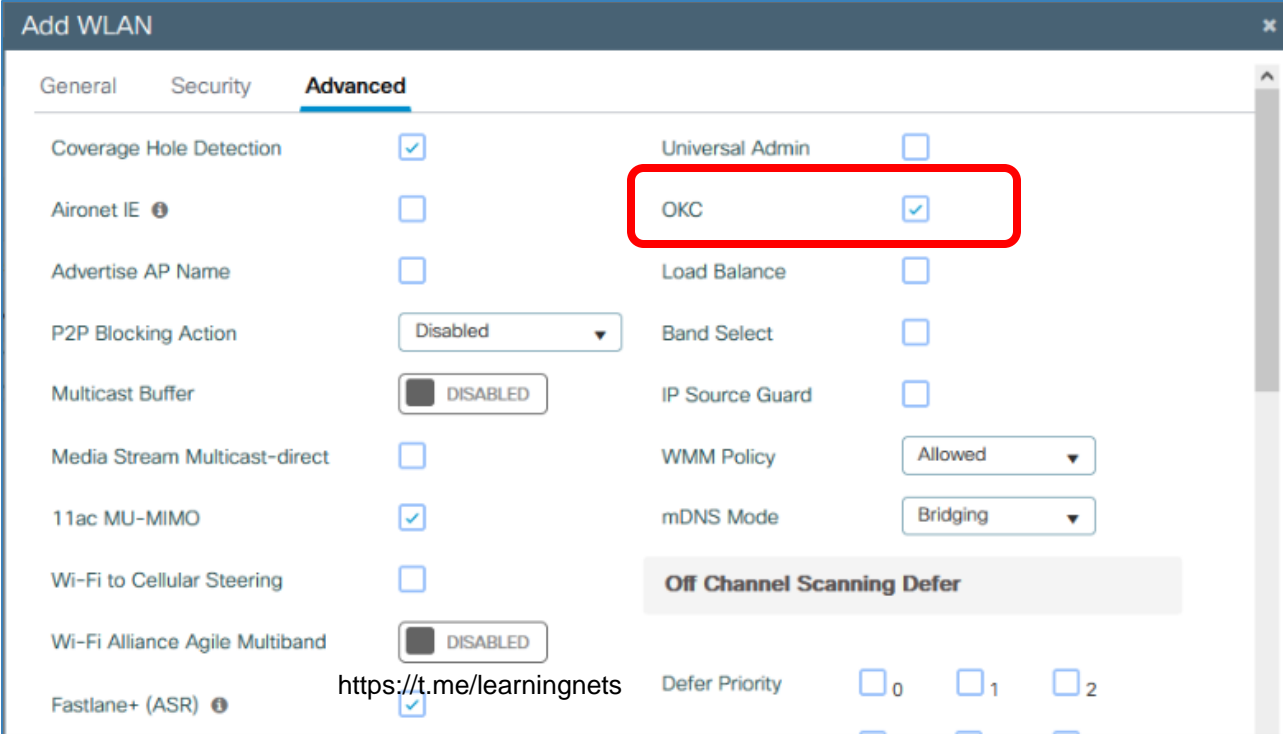


Optimized Roaming with OKC



OKC Configuration

- + OKC is enabled by default when a new WLAN is created in the Cisco Catalyst 9800 WLC



The screenshot shows the 'Add WLAN' configuration page in the Cisco Catalyst 9800 WLC. The 'Advanced' tab is selected, and the 'OKC' checkbox is checked and highlighted with a red box. Other configuration options include Coverage Hole Detection, Aironet IE, Advertise AP Name, P2P Blocking Action, Multicast Buffer, Media Stream Multicast-direct, 11ac MU-MIMO, Wi-Fi to Cellular Steering, Wi-Fi Alliance Agile Multiband, Fastlane+ (ASR), Universal Admin, Load Balance, Band Select, IP Source Guard, WMM Policy, mDNS Mode, and Off Channel Scanning Defer.

Option	Value
Coverage Hole Detection	<input checked="" type="checkbox"/>
Aironet IE	<input type="checkbox"/>
Advertise AP Name	<input type="checkbox"/>
P2P Blocking Action	Disabled
Multicast Buffer	DISABLED
Media Stream Multicast-direct	<input type="checkbox"/>
11ac MU-MIMO	<input checked="" type="checkbox"/>
Wi-Fi to Cellular Steering	<input type="checkbox"/>
Wi-Fi Alliance Agile Multiband	DISABLED
Fastlane+ (ASR)	<input checked="" type="checkbox"/>
Universal Admin	<input type="checkbox"/>
OKC	<input checked="" type="checkbox"/>
Load Balance	<input type="checkbox"/>
Band Select	<input type="checkbox"/>
IP Source Guard	<input type="checkbox"/>
WMM Policy	Allowed
mDNS Mode	Bridging
Off Channel Scanning Defer	
Defer Priority	<input type="checkbox"/> 0 <input type="checkbox"/> 1 <input type="checkbox"/> 2

<https://t.me/learningnets>

OKC Verification

- + OKC is not part of any IEEE standard
- + No specific fields within 802.11 frames to confirm OKC support
- + Look for roaming to WLANs in which 802.1x Radius authentication is skipped but 4-way EAPOL handshake retained

OKC Verification via Sniffer

MotorolaMobi_ba:e6:...	Broadcast	802.11	216	Probe Request, SN=887, FN=0, Flags=.....C, SSID="Dot1x-Test"
Cisco_89:09:ee	MotorolaMobi_ba:e...	802.11	353	Probe Response, SN=3425, FN=0, Flags=.....C, BI=100, SSID="Dot1x-Test"
MotorolaMobi_ba:e6:...	Cisco_89:09:ee	802.11	70	Authentication, SN=923, FN=0, Flags=.....C
Cisco_89:09:ee	MotorolaMobi_ba:e...	802.11	70	Authentication, SN=3426, FN=0, Flags=.....C
MotorolaMobi_ba:e6:...	Cisco_89:09:ee	802.11	290	Reassociation Request, SN=924, FN=0, Flags=.....C, SSID="Dot1x-Test"
Cisco_89:09:ee	MotorolaMobi_ba:e...	802.11	194	Reassociation Response, SN=3427, FN=0, Flags=.....C
Cisco_89:09:ee	MotorolaMobi_ba:e...	EAPOL	193	Key (Message 1 of 4)
MotorolaMobi_ba:e6:...	Cisco_89:09:ee	EAPOL	211	Key (Message 2 of 4)
Cisco_89:09:ee	MotorolaMobi_ba:e...	EAPOL	227	Key (Message 3 of 4)
MotorolaMobi_ba:e6:...	Cisco_89:09:ee	EAPOL	171	Key (Message 4 of 4)



**Thank you for
watching!!**



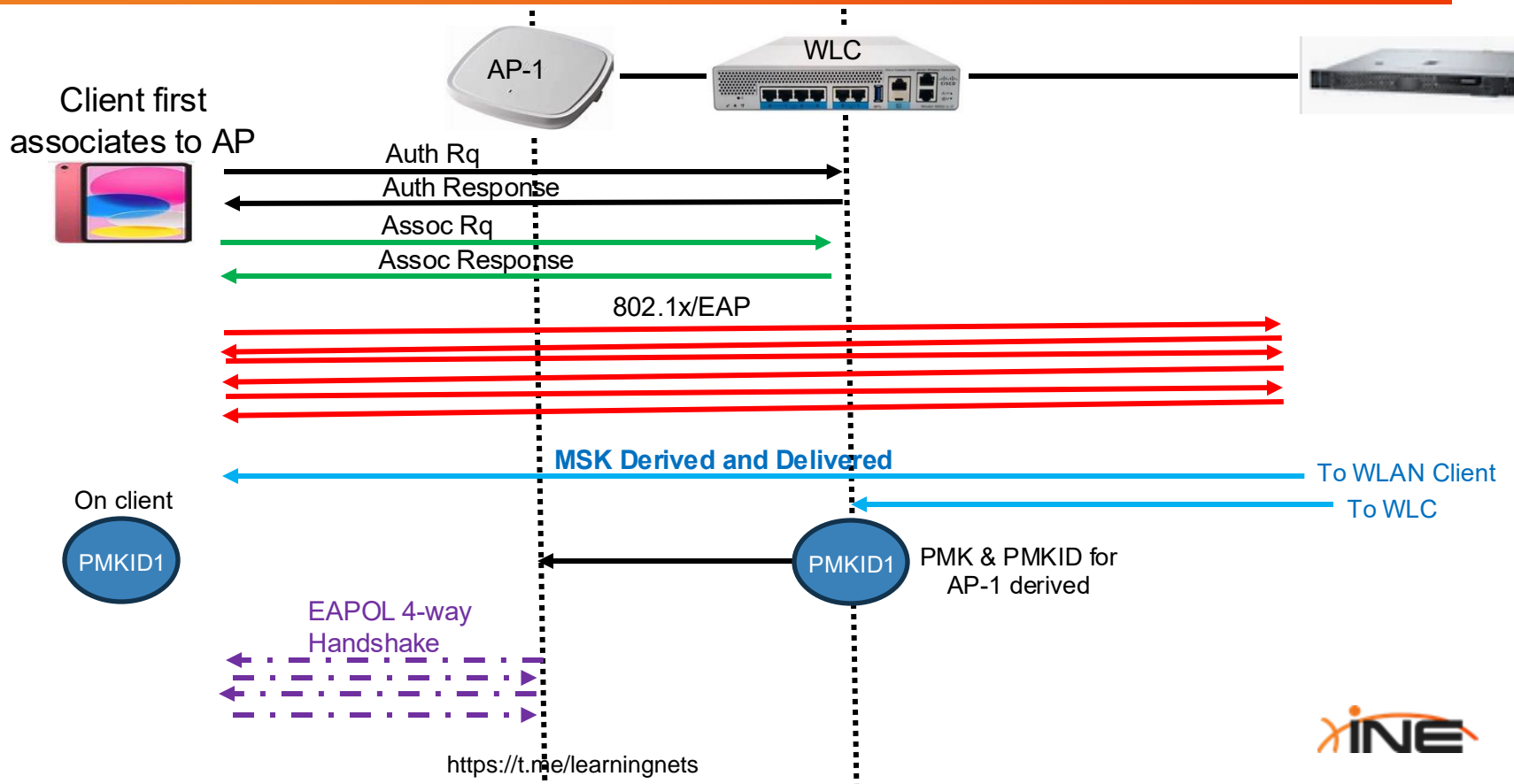
Sticky Key Caching

<https://t.me/learningnets>

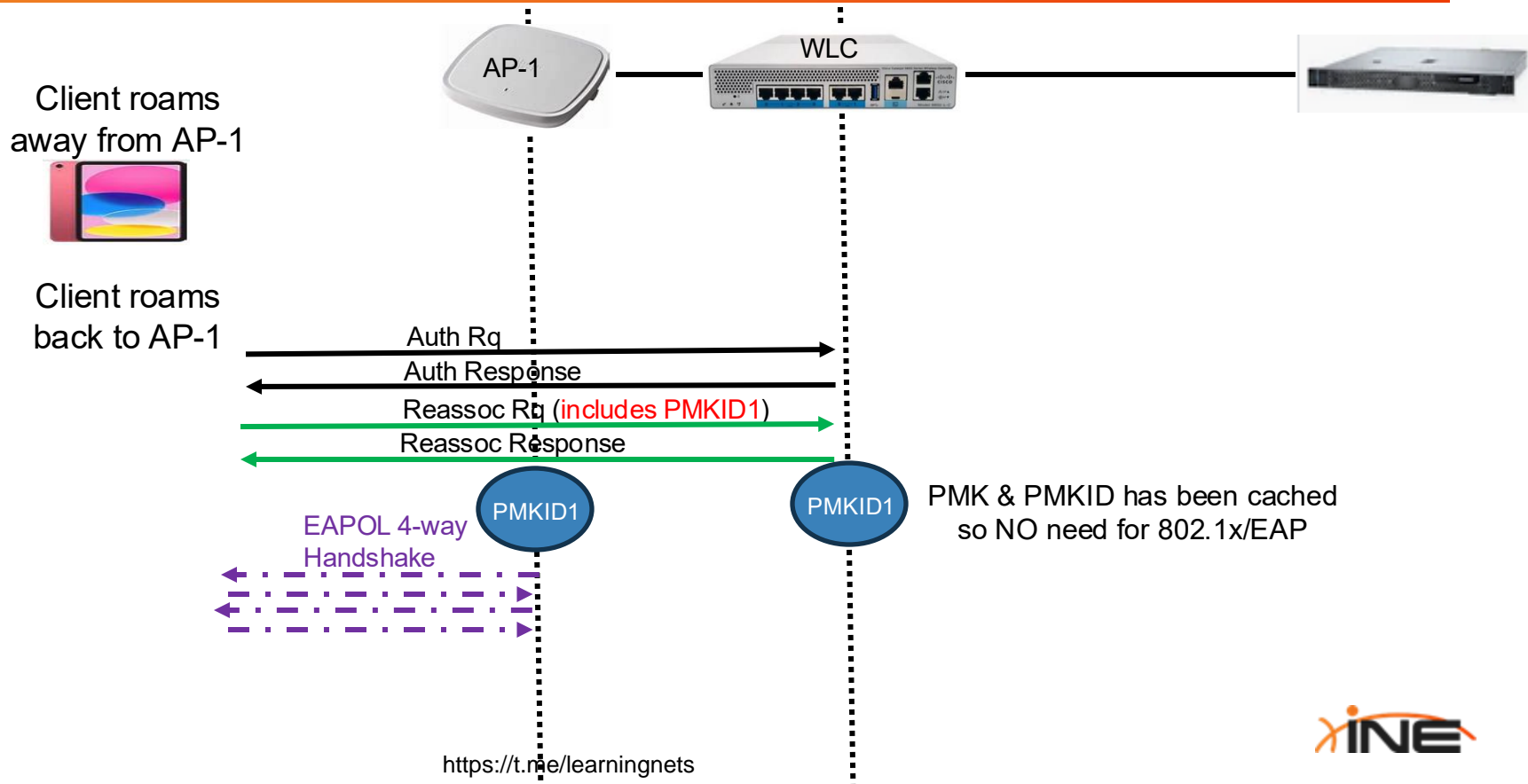
What Problem Did it Solve?

- + Sticky Key Caching was also known as:
 - + Sticky PMKID Caching
 - + PMKID Caching
- + Released in 2004 as part of **802.11i**
- + Designed to eliminate the need for a full 802.1x/EAP exchange *when client roams back to a previously-associated access point*
- + 4-way EAPOL handshake still required

SKC First Association



SKC when Roaming Back



Packet Capture

765	36.431396	MotorolaMobi_ba:e6:...	Cisco_89:09:ee	802.11	70	Authentication, SN=2759, FN=0, Flags=.....C
767	36.432476	Cisco_89:09:ee	MotorolaMobi_ba:e...	802.11	70	Authentication, SN=24, FN=0, Flags=.....C
769	36.436703	MotorolaMobi_ba:e6:...	Cisco_89:09:ee	802.11	70	Authentication, SN=2759, FN=0, Flags=.....C
771	36.438746	MotorolaMobi_ba:e6:...	Cisco_89:09:ee	802.11	290	Reassociation Request, SN=2760, FN=0, Flags=.....C, SSID="Dot1x-Test"
785	36.496262	Cisco_89:09:ee	MotorolaMobi_ba:e...	802.11	194	Reassociation Response, SN=27, FN=0, Flags=.....C
787	36.529288		MotorolaMobi_ba:e...	802.11	68	Clear-to-send, Flags=.....C
789	36.562802	Cisco_89:09:ee	MotorolaMobi_ba:e...	802.11	90	Action, SN=0, FN=0, Flags=.....C
790	36.562870	Cisco_89:09:ee	MotorolaMobi_ba:e...	802.11	90	Action, SN=0, FN=0, Flags=....R...C
791	36.563175	Cisco_89:09:ee	MotorolaMobi_ba:e...	802.11	90	Action, SN=0, FN=0, Flags=....R...C
792	36.563483	Cisco_89:09:ee	MotorolaMobi_ba:e...	802.11	90	Action, SN=0, FN=0, Flags=....R...C
793	36.565920	Cisco_89:09:ee	MotorolaMobi_ba:e...	EAPOL	193	Key (Message 1 of 4)
795	36.577272	MotorolaMobi_ba:e6:...	Cisco_89:09:ee	EAPOL	211	Key (Message 2 of 4)
798	36.637712	Cisco_89:09:ee	MotorolaMobi_ba:e...	EAPOL	227	Key (Message 3 of 4)
800	36.642570	MotorolaMobi_ba:e6:...	Cisco_89:09:ee	EAPOL	171	Key (Message 4 of 4)

```
> Tag: SSID parameter set: "Dot1x-Test"
> Tag: Supported Rates 6(B), 9, 12(B), 18, 24(B), 36, 48, 54, [Mbit/sec]
> Tag: Power Capability Min: 8, Max: 23
> Tag: Supported Channels
v 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
  v Auth Key Management (AKM) List 00:0f:ac (Ieee 802.11) WPA
    v Auth Key Management (AKM) Suite: 00:0f:ac (Ieee 802.11) WPA
      Auth Key Management (AKM) OUI: 00:0f:ac (Ieee 802.11)
      Auth Key Management (AKM) type: WPA (1)
  > RSN Capabilities: 0x0000
  PMKID Count: 1
  v PMKID List
    PMKID: 7489ab9e278a9337a21cfed78ba9fbd1
  > Tag: Supported Operating Classes
  > Tag: HT Capabilities (802.11n D1.10)
  > Tag: Extended Capabilities (8 octets)
  > Tag: VHT Capabilities
```

```
0000 00 00 24 00 6f 08 00 40 2c 49 31
0010 12 0c c8 14 40 01 bb 9f 00 72 00
0020 00 00 00 00 20 00 3c 00 7c 21 0d
0030 51 ba e6 e2 7c 21 0d 89 09 ee 80
0040 78 72 5d 75 9d ce 00 0a 44 6f 74
0050 73 74 01 08 8c 12 98 24 b0 48 60
0060 24 32 24 01 28 01 2c 01 30 01 34
0070 40 01 64 01 68 01 6c 01 70 01 74
0080 80 01 84 01 88 01 8c 01 90 01 95
0090 a1 01 a5 01 30 26 01 00 00 0f ac
00a0 ac 04 01 00 00 0f ac 01 00 00 01
00b0 27 8a 93 37 a2 1c fe d7 8b a9 fb
00c0 53 54 73 74 75 76 77 78 79 7a 7b
00d0 81 83 84 82 2d 1a 6f 08 17 ff ff
00e0 00 00 00 00 00 00 00 00 00 00 00
00f0 7f 08 00 00 00 00 00 00 00 40 bf
0100 fa ff 0c 03 fa ff 0c 23 dd 07 00
0110 00 dd 0b 8c fd f0 01 01 02 01 00
0120 ce 6b
```

SKC Caveats

- + Doesn't work with WPA3 WLANs
- + Doesn't provide any benefit with WPA Personal WLANs
- + WLC will only cache up to 8-PMKs/PMKIDs per client
- + Per Cisco, *"SKC is useful only in cases where you have a small number of clients, which roam among a small number of APs."*
- + Supposedly deprecated but is still operational in Catalyst 9800s



**Thank you for
watching!!**



Understanding 802.11r (Fast BSS Transition)

<https://t.me/learningnets>



The PMK Problem

- + With WPA Enterprise environments
 - + PMK is the essential key from which all other (unicast) keys are derived
 - + Each WLAN client association requires a unique PMK
 - + PMK only derived after full Radius/EAP authentication (or PSK/SAE authentication)
 - + Full Radius/EAP authentication required each time after roaming
- + All of these authentication steps required before deriving PMK can induce roaming latency

What is 802.11r (Fast BSS Transition)?

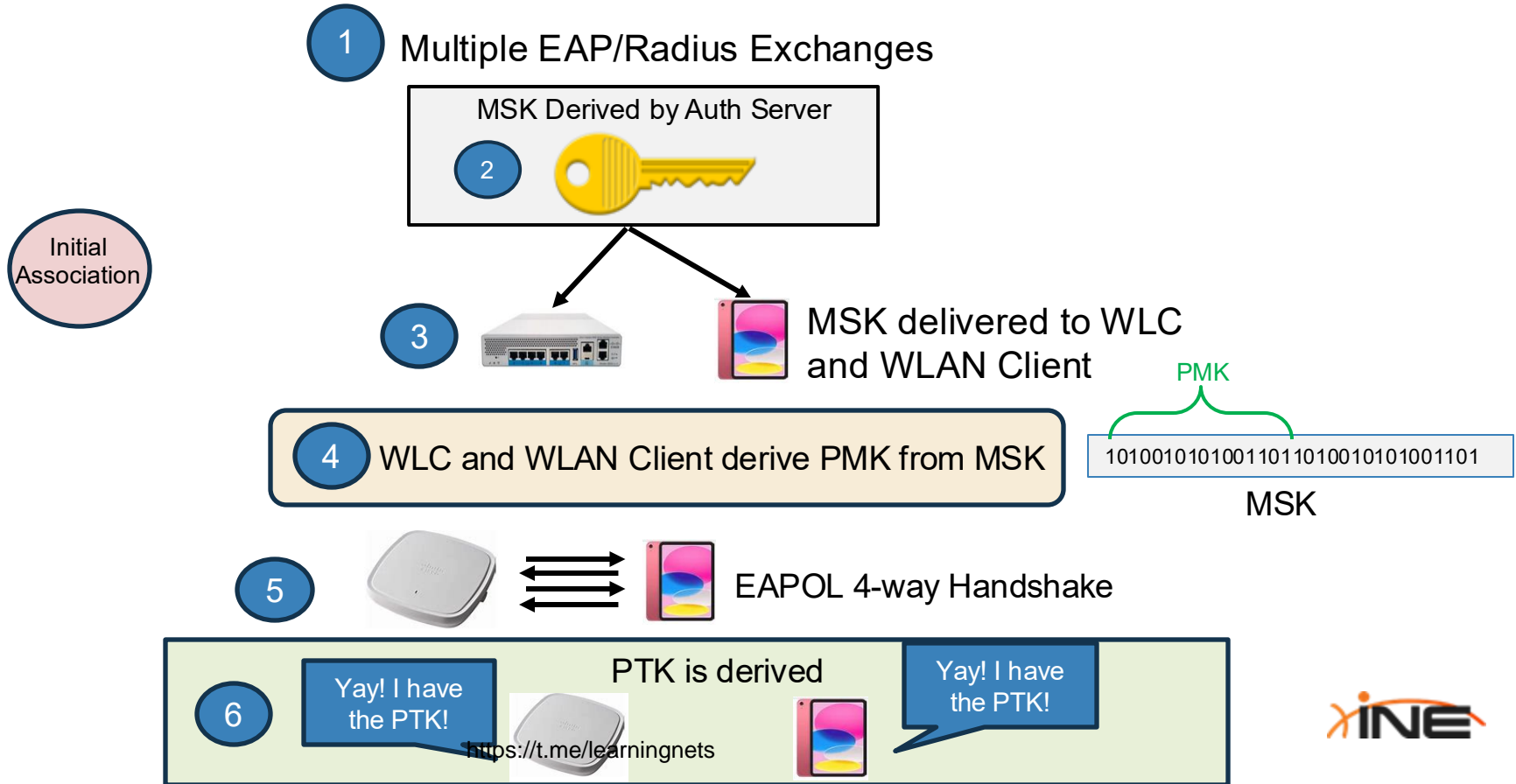
- + Defined by IEEE 802.11r standard (FT = Fast Transition)
- + Enables fast and secure client roaming between access points by;
 - + Pre-establishing a key hierarchy
 - + Optimizing handoffs
 - + Eliminating the need for full reauthentication at every AP.
- + Works with both WPA2-Enterprise (EAP) and WPA2/WPA3-Personal
- + Must be supported by both WLAN Client and access point (or Controller)



How Does Fast BSS Transition Work?

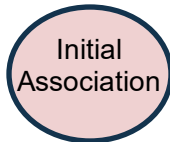
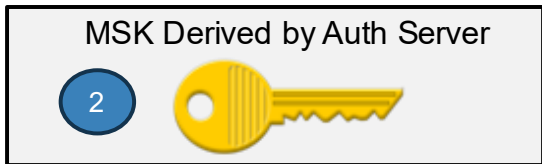
- + Creates a new hierarchy of keys
- + Pre-derived keys can be used at the target AP during roaming event without full re-authentication.
 - + *Avoids full Radius/EAP exchange with Enterprise WLANs*
 - + *Avoids SAE exchange with WPA-3 Personal WLANs*
 - + *Avoids 4-Way EAPOL Handshake in all cases*
- + Controller sends derived keys to surrounding APs that the WLAN client is in the process of roaming to.

Enterprise Key Hierarchy w/o FT



Enterprise Key Hierarchy with FT

1 Multiple EAP/Radius Exchanges



3 MSK delivered to WLC and WLAN Client



4 WLC and WLAN Client derive **PMK-R0** from MSK


5 WLC derives **PMK-R1** value from PMK-R0 for specific AP client is connecting to and distributes it to AP.



PMKR1 #1

AP-1

6 Client independently derives **PMK-R1** value for AP it is associating to.



7 EAPOL 4-way Handshake using **PMKR1** derives PTK



Roaming with FT

- + When WLAN clients roam with 802.11r the 802.11 “Authentication” message is modified
- + The new Authentication message includes;
 - + “Fast BSS Transition” as “*authentication algorithm*”
 - + “Mobility Domain” information
 - + Various nonces
 - + PMK-R0 key holder information
- + This new message is termed, “*FT Request*”
- + AP/WLC responds with “*FT Response*”

802.11 Authentication Message w/o FT

	Destination	Protocol	Length	Info
	Cisco_75:9d:cf	802.11	70	Acknowledgement, P...
:08:38:9d:b5	Cisco_75:9d:cf	802.11	70	Authentication, SN=2

- > Frame 663: 70 bytes on wire (560 bits), 70 bytes captured (560 bits)
- > Radiotap Header v0, Length 36
- > 802.11 radio information
- > IEEE 802.11 Authentication, Flags:C
- ✓ IEEE 802.11 Wireless Management
 - ✓ Fixed parameters (6 bytes)
 - Authentication Algorithm: Open System (0)
 - Authentication SEQ: 0x0001
 - Status code: Successful (0x0000)

FT Request from WLAN Client

New Fields
added by
802.11r (FT)

```
08:38:9d:b5 Cisco_89:09:ef 802.11 205 Authentication, SN=863, FN=0, F
> Frame 417: 205 bytes on wire (1640 bits), 205 bytes captured (1640 bits)
> Radiotap Header v0, Length 36
> 802.11 radio information
> IEEE 802.11 Authentication, Flags: .....C
v IEEE 802.11 Wireless Management
  v Fixed parameters (6 bytes)
    Authentication Algorithm: Fast BSS Transition (2)
    Authentication SEQ: 0x0001
    Status code: Successful (0x0000)
  v Tagged parameters (135 bytes)
    v 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
      v Auth Key Management (AKM) List 00:0f:ac (Ieee 802.11) FT using PSK
        v Auth Key Management (AKM) Suite: 00:0f:ac (Ieee 802.11) FT using PSK
          Auth Key Management (AKM) OUI: 00:0f:ac (Ieee 802.11)
          Auth Key Management (AKM) type: FT using PSK (4)
      > RSN Capabilities: 0x0080
      PMKID Count: 1
      > PMKID List
    v Tag: Mobility Domain
      Tag Number: Mobility Domain (54)
      Tag length: 3
      Mobility Domain Identifier: 0x34ac
      > FT Capability and Policy: 0x00
    v Tag: Fast BSS Transition
      Tag Number: Fast BSS Transition (55)
      Tag length: 88
      > MIC Control: 0x0000
      MIC: 00000000000000000000000000000000
      ANonce: 0000000000000000000000000000000000000000000000000000000000000000
      SNonce: 954d49ab9dae4d5d31776b4775efd5783f1a5a8508189ab75124305e73cdeb54
```



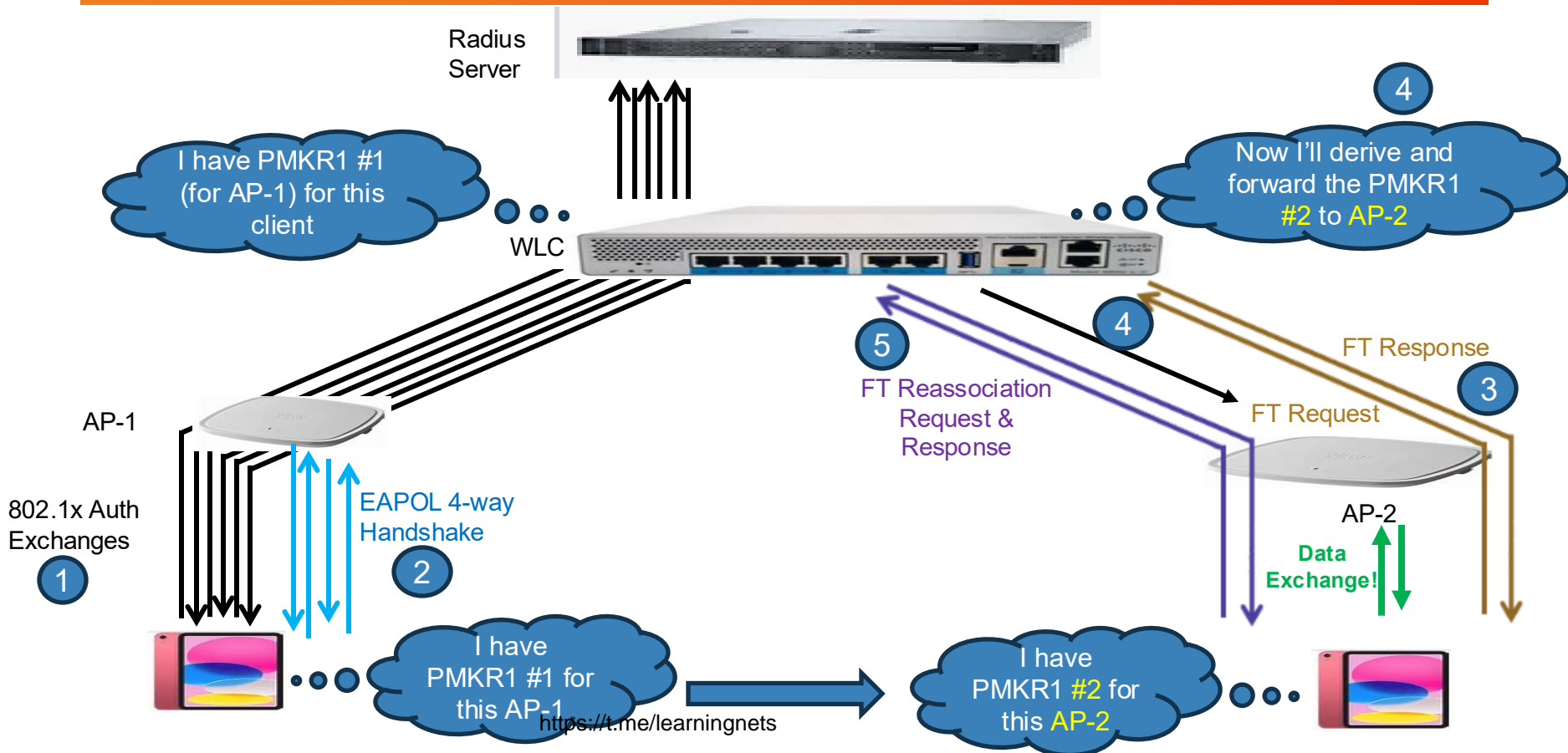
FT Response from Access Point

```
Cisco_89:09:ef 0a:c2:08:38:9d:b5 802.11 213 Authentication, SN=31, F
> Radiotap Header v0, Length 36
> 802.11 radio information
> IEEE 802.11 Authentication, Flags: .....C
> IEEE 802.11 Wireless Management
  > Fixed parameters (6 bytes)
    Authentication Algorithm: Fast BSS Transition (2)
    Authentication SEQ: 0x0002
    Status code: Successful (0x0000)
  > Tagged parameters (143 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 using PSK
      > RSN Capabilities: 0x0028
        PMKID Count: 1
      > PMKID List
    > Tag: Mobility Domain
  > Tag: Fast BSS Transition
    Tag Number: Fast BSS Transition (55)
    Tag length: 96
    > MIC Control: 0x0000
    MIC: 00000000000000000000000000000000
    ANonce: e56cb9e56ae0421e82794c96897a20038fac2abee19b6acc1454c312024a471e
    SNonce: 954d49ab9dae4d5d31776b4775efd5783f1a5a8508189ab75124305e73cdeb54
  > 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): e51a4fe52768
  > Subelement: PMK-R0 key holder identifier (R0KH-ID)
    Subelement ID: PMK-R0 key holder identifier (R0KH-ID) (3)
    Length: 18
    PMK-R0 key holder identifier (R0KH-ID): 459a4ce9
```

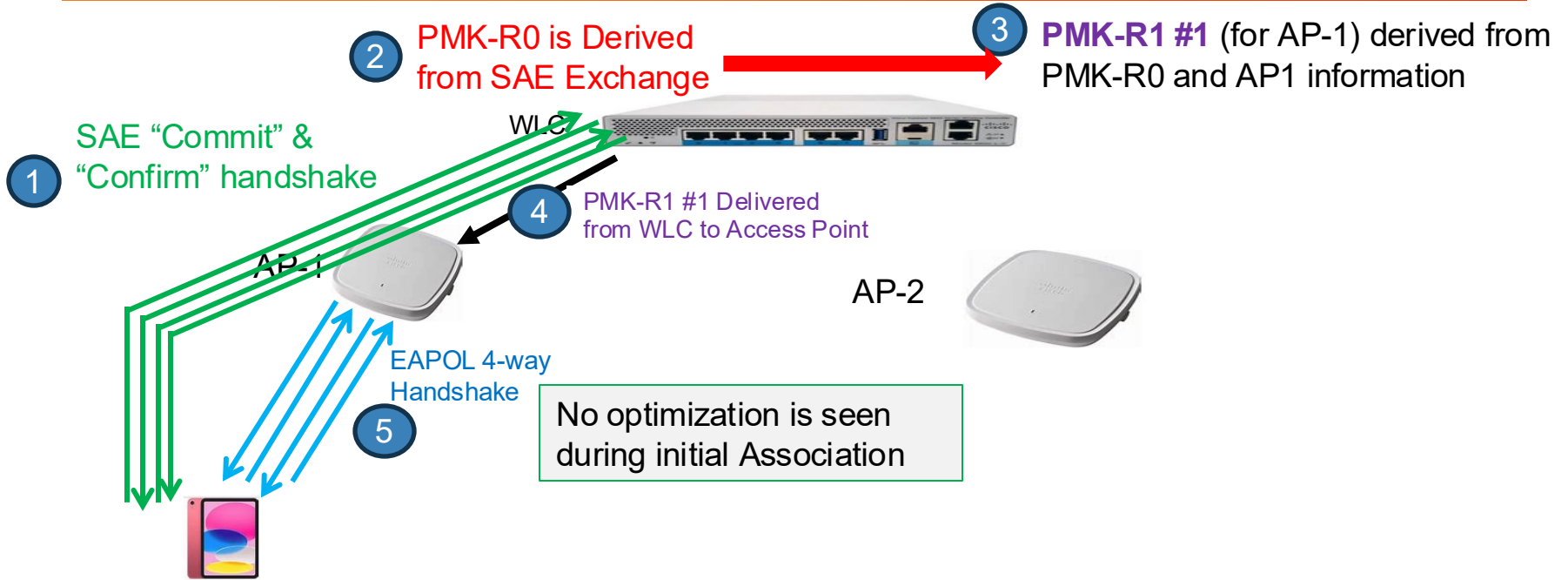
Notice the AP/WLC provides the PMK-R1 Key Holder ID



How Does 802.11r Help WPA-Enterprise Roaming?



802.11r Modifications with WPA-3 SAE (1)



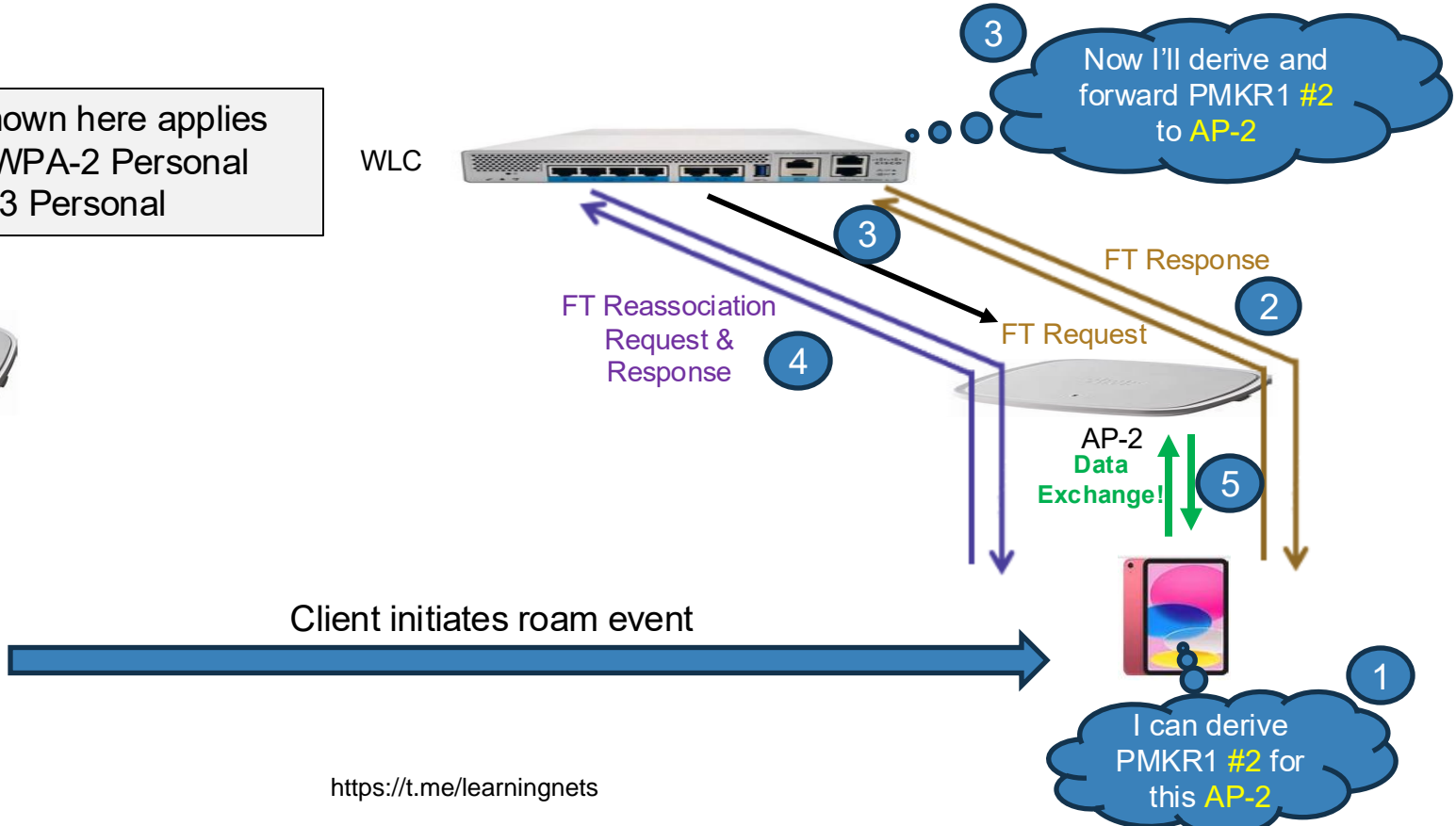
2 PMK-R0 is Derived from SAE exchange → 3 PMK-R1 #1 (for AP-1) derived from PMK-R0 and AP1 information

1 Authentication with SAE is completed.

4 802.11 Association Message exchange. <https://t.me/learningnets>

802.11r Optimization with WPA Personal

What is shown here applies with both WPA-2 Personal and WPA-3 Personal





**Thank you for
watching!!**



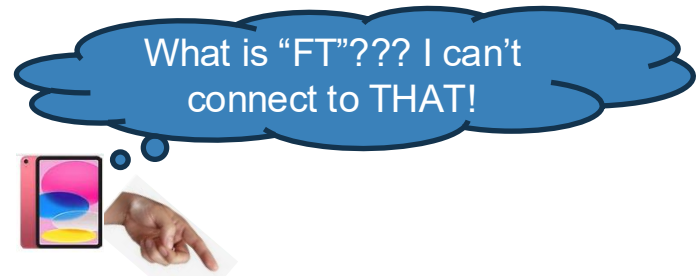
Fast Transition Modes

<https://t.me/learningnets>



The Problem with Legacy Clients

- + WLANs can have a mixture of legacy and newer clients
- + Legacy WLAN clients may not understand 802.11r FT AKM methods advertised in beacons and not be able to connect
- + Three configurable modes of FT exist to best suit your WLAN client environment:
 - + FT Only
 - + FT Adaptive Mode
 - + FT Mixed Mode



Auth Key Management (AKM) List 00:0f:ac (Ieee 802.11) FT over IEEE 802.1X

FT Only Mode

- + Advertises FT-capable AKM method in Beacons and Probe Responses
- + Includes Mobility Domain ID
- + Only useful when **all** WLAN clients support 802.11r

FT Only Mode

```
> IEEE 802.11 Beacon frame, Flags: .....C
v IEEE 802.11 Wireless Management
  > Fixed parameters (12 bytes)
  v Tagged parameters (290 bytes)
    v Tag: SSID parameter set: "Dot1x-Test"
      Tag Number: SSID parameter set (0)
      Tag length: 10
      SSID: "Dot1x-Test"
    > Tag: Supported Rates 6(B), 9, 12(B), 18, 24(B), 36, 48, 54, [Mbit/sec]
    > Tag: DS Parameter set: Current Channel: 116
    > Tag: Traffic Indication Map (TIM): DTIM 0 of 1 bitmap
    > Tag: Country Information: Country Code US, Environment All
    > Tag: Power Constraint: 0
    v 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
      v Auth Key Management (AKM) List 00:0f:ac (Ieee 802.11) FT over IEEE 802.1X
        v Auth Key Management (AKM) Suite: 00:0f:ac (Ieee 802.11) FT over IEEE 802.1X
          Auth Key Management (AKM) OUI: 00:0f:ac (Ieee 802.11)
          Auth Key Management (AKM) type: FT over IEEE 802.1X (3)
      > RSN Capabilities: 0x0028
    > Tag: QBSS Load Element 802.11e CCA Version
    v Tag: Mobility Domain
      Tag Number: Mobility Domain (54)
      Tag length: 3
      Mobility Domain ID: 0x00000000
      > FT Capability and Policy: 0x00
```

FT Adaptive Mode

- + Designed to allow FT and non-FT capable devices on the same SSID.
- + Developed by Cisco in partnership with device ecosystems partners like Apple and Samsung
- + Beacon does not advertise the FT AKM at all, but will use FT when supported clients connect
 - + Still advertises Mobility Domain tag
- + In the C9800, Adaptive FT is enabled by default.
- + *Adaptive FT does not support WPA-3 WLANs*

FT Adaptive Mode (Enterprise)

```
> IEEE 802.11 Beacon frame, Flags: .....C
  > IEEE 802.11 Wireless Management
    > Fixed parameters (12 bytes)
    > Tagged parameters (290 bytes)
      > Tag: SSID parameter set: "Dot1x-Test"
        Tag Number: SSID parameter set (0)
        Tag length: 10
        SSID: "Dot1x-Test"
      > Tag: Supported Rates 6(B), 9, 12(B), 18, 24(B), 36, 48, 54, [Mbit/sec]
      > Tag: DS Parameter set: Current Channel: 116
      > Tag: Traffic Indication Map (TIM): DTIM 0 of 1 bitmap
      > Tag: Country Information: Country Code US, Environment All
      > Tag: Power Constraint: 0
      > 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) WPA
          > Auth Key Management (AKM) Suite: 00:0f:ac (Ieee 802.11) WPA
            Auth Key Management (AKM) OUI: 00:0f:ac (Ieee 802.11)
            Auth Key Management (AKM) type: WPA (1)
        > RSN Capabilities: 0x0028
      > Tag: QBSS Load Element 802.11e CCA Version
      > Tag: Mobility Domain
        Tag Number: Mobility Domain (54)
        Tag length: 3
        Mobility Domain Name: 0x34ac
        > FT Capability and Policy: 0x00
```

FT-capable clients will understand "Mobility Domain"

No mention of "FT" within AKM methods.

"WPA" displayed on WPA Enterprise WLANs



FT Adaptive Mode (Personal)

```
> IEEE 802.11 Beacon frame, Flags: .....C
< IEEE 802.11 Wireless Management
  > Fixed parameters (12 bytes)
  < Tagged parameters (294 bytes)
    < Tag: SSID parameter set: "WPA-PSK"
      Tag Number: SSID parameter set (0)
      Tag length: 7
      SSID: "WPA-PSK"
    > Tag: Supported Rates 6(B), 9, 12(B), 18, 24(B), 36, 48, 54, [Mbit/sec]
    > Tag: DS Parameter set: Current Channel: 116
    > Tag: Traffic Indication Map (TIM): DTIM 0 of 1 bitmap
    > Tag: Country Information: Country Code US, Environment All
    > Tag: Power Constraint: 0
    < 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) PSK
        < Auth Key Management (AKM) Suite: 00:0f:ac (Ieee 802.11) PSK
          Auth Key Management (AKM) OUI: 00:0f:ac (Ieee 802.11)
          Auth Key Management (AKM) type: PSK (2)
        > RSN Capabilities: 0x0028
      > Tag: QoS Load Element 802.11e CCA version
      > Tag: RM Enabled Capabilities (5 octets)
    < Tag: Mobility Domain
      Tag Number: Mobility Domain (54)
      Tag length: 3
      Mobility Domain Name: https://t.me/learningnets34ac
      > FT Capability and Policy: 0x00
```

"PSK" displayed
on WPA Personal
WLANs



FT Mixed Mode

- + Advertises both FT-capable and legacy AKM methods
- + Some legacy clients still get confused over the presence of FT AKM methods
- + Cisco TAC recommends using “Mixed Mode” as issues still persist with “Adaptive Mode”

FT Mixed Mode

```
> IEEE 802.11 Beacon frame, Flags: .....C
v IEEE 802.11 Wireless Management
  > Fixed parameters (12 bytes)
  v Tagged parameters (294 bytes)
    v Tag: SSID parameter set: "Dot1x-Test"
      Tag Number: SSID parameter set (0)
      Tag length: 10
      SSID: "Dot1x-Test"
    > Tag: Supported Rates 6(B), 9, 12(B), 18, 24(B), 36, 48, 54, [Mbit/sec]
    > Tag: DS Parameter set: Current Channel: 116
    > Tag: Traffic Indication Map (TIM): DTIM 0 of 1 bitmap
    > Tag: Country Information: Country Code US, Environment All
    > Tag: Power Constraint: 0
    v 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
    v Auth Key Management (AKM) List 00:0f:ac (Ieee 802.11) WPA 00:0f:ac (Ieee 802.11) FT over IEEE 802.1X
      v Auth Key Management (AKM) Suite: 00:0f:ac (Ieee 802.11) WPA
        Auth Key Management (AKM) OUI: 00:0f:ac (Ieee 802.11)
        Auth Key Management (AKM) type: WPA (1)
      v Auth Key Management (AKM) Suite: 00:0f:ac (Ieee 802.11) FT over IEEE 802.1X
        Auth Key Management (AKM) OUI: 00:0f:ac (Ieee 802.11)
        Auth Key Management (AKM) type: FT over IEEE 802.1X (3)
    > RSN Capabilities: 0x0028
  > Tag: QBSS Load Element 802.11e CCA Version
  v Tag: Mobility Domain
    Tag Number: Mobility Domain (54)
    Tag length: 3
    Mobility Domain Identifier: https://t.me/learningnets
  > FT Capability and Policy: 0x00
```



So What is Best?

From the document “Cisco Catalyst 9800 Series Configuration Best Practices”

The reality is that in a mixed-client network, some non-FT clients may experience issues in connecting to a WLAN with Adaptive FT, so the recommendation from Cisco is to configure a single WLAN with “802.11r mixed mode”, to allow for compatibility between 802.11r and non-802.11r clients

ii. 802.11r (fast transition) – can sometimes be problematic. See [9800 best practices guide](#) for more info. 802.11r “mixed-mode” is now considered best practice. Still the occasional issue even with mixed-mode but generally has been better than Adaptive FT.

Adaptive Mode with Motorola

```
765 36.431396 MotorolaMobi_ba:e6:... Cisco_89:09:ee 802.11 70 Authentication, SN=2759, FN=0, Flags=.....C
767 36.432476 Cisco_89:09:ee MotorolaMobi_ba:e... 802.11 70 Authentication, SN=24, FN=0, Flags=.....C
769 36.436703 MotorolaMobi_ba:e6:... Cisco_89:09:ee 802.11 70 Authentication, SN=2759, FN=0, Flags=.....C
771 36.438746 MotorolaMobi_ba:e6:... Cisco_89:09:ee 802.11 290 Reassociation Request, SN=2760, FN=0, Flags=.....C, SSID="Dot1x-Test"
785 36.496262 Cisco_89:09:ee MotorolaMobi_ba:e... 802.11 194 Reassociation Response, SN=27, FN=0, Flags=.....C
787 36.529288 MotorolaMobi_ba:e... 802.11 68 Clear-to-send, Flags=.....C
789 36.562802 Cisco_89:09:ee MotorolaMobi_ba:e... 802.11 90 Action, SN=0, FN=0, Flags=.....C
790 36.562870 Cisco_89:09:ee MotorolaMobi_ba:e... 802.11 90 Action, SN=0, FN=0, Flags=....R...C
791 36.563175 Cisco_89:09:ee MotorolaMobi_ba:e... 802.11 90 Action, SN=0, FN=0, Flags=....R...C
792 36.563483 Cisco_89:09:ee MotorolaMobi_ba:e... 802.11 90 Action, SN=0, FN=0, Flags=....R...C
793 36.565920 Cisco_89:09:ee MotorolaMobi_ba:e... EAPOL 193 Key (Message 1 of 4)
795 36.577272 MotorolaMobi_ba:e6:... Cisco_89:09:ee EAPOL 211 Key (Message 2 of 4)
798 36.637712 Cisco_89:09:ee MotorolaMobi_ba:e... EAPOL 227 Key (Message 3 of 4)
800 36.642570 MotorolaMobi_ba:e6:... Cisco_89:09:ee EAPOL 171 Key (Message 4 of 4)
```

```
> Tag: SSID parameter set: "Dot1x-Test"
> Tag: Supported Rates 6(B), 9, 12(B), 18, 24(B), 36, 48, 54, [Mbit/sec]
> Tag: Power Capability Min: 8, Max: 23
> Tag: Supported Channels
v 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
    v Auth Key Management (AKM) List 00:0f:ac (Ieee 802.11) WPA
      v Auth Key Management (AKM) Suite: 00:0f:ac (Ieee 802.11) WPA
        Auth Key Management (AKM) OUI: 00:0f:ac (Ieee 802.11)
        Auth Key Management (AKM) type: WPA (1)
  > RSN Capabilities: 0x0000
  PMKID Count: 1
  v PMKID List
    PMKID: 7489ab9e278a9337a21cfd78ba9fbd1
  > Tag: Supported Operating Classes
  > Tag: HT Capabilities (802.11n D1.10)
  > Tag: Extended Capabilities (8 octets)
  > Tag: VHT Capabilities
```

```
0000 00 00 24 00 6f 08 00 40 2c 49 31
0010 12 0c c8 14 40 01 bb 9f 00 72 00
0020 00 00 00 00 20 00 3c 00 7c 21 0d
0030 51 ba e6 e2 7c 21 0d 89 09 ee 80
0040 78 72 5d 75 9d ce 00 0a 44 6f 74
0050 73 74 01 08 8c 12 98 24 b0 48 60
0060 24 32 24 01 28 01 2c 01 30 01 34
0070 40 01 64 01 68 01 6c 01 70 01 74
0080 80 01 84 01 88 01 8c 01 90 01 95
0090 a1 01 a5 01 30 26 01 00 00 0f ac
00a0 ac 04 01 00 00 0f ac 01 00 00 01
00b0 27 8a 93 37 a2 1c fe d7 8b a9 fb
00c0 53 54 73 74 75 76 77 78 79 7a 7b
00d0 81 83 84 82 2d 1a 6f 08 17 ff ff
00e0 00 00 00 00 00 00 00 00 00 00 00
00f0 7f 08 00 00 00 00 00 00 00 40 bf
0100 fa ff 0c 03 fa ff 0c 23 dd 07 00
0110 00 dd 0b 8c fd f0 01 01 02 01 00
0120 ce 6b
```

Adaptive Mode with Apple iPad

```

> IEEE 802.11 Reassociation Request, Flags: .....C
v IEEE 802.11 Wireless Management
  > Fixed parameters (10 bytes)
  v Tagged parameters (259 bytes)
    v Tag: SSID parameter set: "Dot1x-Test"
      Tag Number: SSID parameter set (0)
      Tag length: 10
      SSID: "Dot1x-Test"
    > Tag: Supported Rates 6(B), 9, 12(B), 18, 24(B), 36, 48, 54, [Mbit/sec]
    > Tag: Power Capability Min: -7, Max: 18
    > Tag: Supported Channels
    v 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
    v Auth Key Management (AKM) List 00:0f:ac (Ieee 802.11) FT over IEEE 802.1X
      v Auth Key Management (AKM) Suite: 00:0f:ac (Ieee 802.11) FT over IEEE 802.1X
        Auth Key Management (AKM) OUI: 00:0f:ac (Ieee 802.11)
        Auth Key Management (AKM) type: FT over IEEE 802.1X (3)
    > RSN Capabilities: 0x000c
      PMKID Count: 1
    v PMKID List
      PMKID: 9f7cfbb716db993c3ebbd9d6c76b6ed4
  v Tag: Mobility Domain
    Tag Number: Mobility Domain (54)
    Tag length: 3
    Mobility Domain Identifier: 0x34ac
  > FT Capability and Policy: 0x00
  v Tag: Fast BSS Transition

```



**Thank you for
watching!!**



Configuring & Verifying Fast BSS Transition (802.11r)

<https://t.me/learningnets>



Enabling 802.11r on the Catalyst 9800

+ 802.11r is typically enabled by default, but if not...

The screenshot shows the 'Edit WLAN' configuration page for a Catalyst 9800. The 'Security' tab is selected, and the 'Layer2' sub-tab is active. The 'WPA + WPA2' radio button is selected. The 'Fast Transition' section has a dropdown menu open, showing 'Disabled' selected, with 'Enabled' and 'Adaptive Enabled' also visible. A red arrow points to this dropdown. The 'Auto Key Mgmt' section is highlighted with a blue box, and the 'FT + 802.1X' checkbox is checked, with a red arrow pointing to it. Other checkboxes include '802.1X', 'Easy-PSK', 'PSK', 'CCKM', 'PSK-SHA256', 'WPA Policy', 'WPA2 Policy', 'GTK Randomize', 'OSEN Policy', 'AES(CCMP128)', 'GCMP128', 'CCMP256', and 'GCMP256'. A warning message at the top states: 'Changing WLAN parameters while it is enabled will result in loss of connectivity for clients connected to it.'

<https://t.me/learningnets>



Packet Capture: 802.11r Initial Association

Source	Destination	Protocol	Length	Info
da:ff:ce:28:22:b8	Cisco_75:9d:ce	802.11	70	Authentication, SN=3189, FN=0, Flags=.....C
Cisco_75:9d:ce	da:ff:ce:28:22:b8	802.11	70	Authentication, SN=2617, FN=0, Flags=.....C
da:ff:ce:28:22:b8	Cisco_75:9d:ce	802.11	342	Association Request, SN=3190, FN=0, Flags=.....C, SSID="Dot1x-Test"
Cisco_75:9d:ce	da:ff:ce:28:22:b8	802.11	292	Association Response, SN=2618, FN=0, Flags=.....C
Cisco_75:9d:ce	da:ff:ce:28:22:b8	EAP	81	Request, Identity
da:ff:ce:28:22:b8	Cisco_75:9d:ce	EAP	84	Response, Identity
Cisco_75:9d:ce	da:ff:ce:28:22:b8	EAP	82	Request, TLS EAP (EAP-TLS)
da:ff:ce:28:22:b8	Cisco_75:9d:ce	EAP	82	Response, Legacy Nak (Response Only)
Cisco_75:9d:ce	da:ff:ce:28:22:b8	EAP	82	Request, Protected EAP (EAP-PEAP)
da:ff:ce:28:22:b8	Cisco_75:9d:ce	TLSv1.2	213	Client Hello
00:00:00_00:00:00	00:00:00_00:00:00	802.11	67	Association Request, SN=2619, FN=0, Flags=.....C[Malformed Packet]
Cisco_75:9d:ce	da:ff:ce:28:22:b8	EAP	1088	Request, Protected EAP (EAP-PEAP)
da:ff:ce:28:22:b8	Cisco_75:9d:ce	EAP	82	Response, Protected EAP (EAP-PEAP)
Cisco_75:9d:ce	da:ff:ce:28:22:b8	EAP	1084	Request, Protected EAP (EAP-PEAP)
da:ff:ce:28:22:b8	Cisco_75:9d:ce	EAP	82	Response, Protected EAP (EAP-PEAP)
Cisco_75:9d:ce	da:ff:ce:28:22:b8	TLSv1.2	151	Server Hello, Certificate, Server Key Exchange, Server Hello Done
da:ff:ce:28:22:b8	Cisco_75:9d:ce	TLSv1.2	240	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
Cisco_75:9d:ce	da:ff:ce:28:22:b8	TLSv1.2	133	Change Cipher Spec, Encrypted Handshake Message
da:ff:ce:28:22:b8	Cisco_75:9d:ce	EAP	82	Response, Protected EAP (EAP-PEAP)
Cisco_75:9d:ce	da:ff:ce:28:22:b8	TLSv1.2	116	Application Data
da:ff:ce:28:22:b8	Cisco_75:9d:ce	TLSv1.2	122	Application Data

Full
Radius/EAP
Exchange

Packet Capture: 802.11r Roam

Source	Destination	Protocol	Length	Info
da:ff:ce:28:22:b8	Cisco_89:09:ee	802.11	205	Authentication, SN=3555, FN=0, Flags=.....C
Cisco_89:09:ee	da:ff:ce:28:22:b8	802.11	213	Authentication, SN=876, FN=0, Flags=.....C
da:ff:ce:28:22:b8	Cisco_89:09:ee	802.11	439	Reassociation Request, SN=3556, FN=0, Flags=.....C, SSID="Dot1x-Test"
Cisco_89:09:ee	da:ff:ce:28:22:b8	802.11	369	Reassociation Response, SN=877, FN=0, Flags=.....C
da:ff:ce:28:22:b8	Cisco_89:09:ee	802.11	73	Action, SN=0, FN=0, Flags=.....C, Dialog Token=1
Cisco_89:09:ee	da:ff:ce:28:22:b8	802.11	73	Action, SN=0, FN=0, Flags=.....C, Dialog Token=1
Cisco_89:09:ee	da:ff:ce:28:22:b8	802.11	68	802.11 Block Ack, Flags=.....C
Cisco_89:09:ee	da:ff:ce:28:22:b8	802.11	68	802.11 Block Ack, Flags=.....C
Cisco_89:09:ee	da:ff:ce:28:22:b8	802.11	90	Action, SN=1, FN=0, Flags=.....C
da:ff:ce:28:22:b8	Broadcast	802.11	116	QoS Data, SN=2, FN=0, Flags=.p.....TC
da:ff:ce:28:22:b8	aa:bb:cc:80:50:00	802.11	116	QoS Data, SN=3, FN=0, Flags=.p.....TC

No 802.1x or EAPOL after roaming!!

Verifying AP Support for 802.11r

```
_75:9d:cf      Broadcast      802.11      370 Beacon frame, SN=3995, FN=0, Flags=.....C, B
```

```
> 802.11 radio information
> IEEE 802.11 Beacon frame, Flags: .....C
v IEEE 802.11 Wireless Management
  v Fixed parameters (12 bytes)
    Timestamp: 11368345611
    Beacon Interval: 0.102400 [Seconds]
    > Capabilities Information: 0x1111
  v Tagged parameters (294 bytes)
    v Tag: SSID parameter set: "WPA-PSK"
      Tag Number: SSID parameter set (0)
      Tag length: 7
      SSID: "WPA-PSK"
    > Tag: Supported Rates 6(B), 9, 12(B), 18, 24(B), 36, 48, 54, [Mbit/sec]
    > Tag: DS Parameter set: Current Channel: 100
    > Tag: Traffic Indication Map (TIM): DTIM 0 of 1 bitmap
    > Tag: Country Information: Country Code US, Environment All
    > Tag: Power Constraint: 0
    > Tag: RSN Information
    > Tag: QBSS Load Element 802.11e CCA Version
    > Tag: RM Enabled Capabilities (5 octets)
    v Tag: Mobility Domain
      Tag Number: Mobility Domain (54)
      Tag length: 3
      Mobility Domain Identifier: 0x34ac
    > FT Capability and Policy: 0x00
```

<https://t.me/learningnets>

Verifying Client Support for 802.11r

Destination	Protocol	Length	Info
:08:38:9d:b5	Cisco_75:9d:cf	802.11	273 Association Request, SN=2215


```
> Frame 152: 273 bytes on wire (2184 bits), 273 bytes captured (2184 bits)
> Radiotap Header v0, Length 36
> 802.11 radio information
> IEEE 802.11 Association Request, Flags: .....C
  > IEEE 802.11 Wireless Management
    > Fixed parameters (4 bytes)
      > Capabilities Information: 0x1111
        Listen Interval: 0x0001
    > Tagged parameters (205 bytes)
      > Tag: SSID parameter set: "WPA-PSK"
      > Tag: Supported Rates 6(B), 9, 12(B), 18, 24(B), 36, 48, 54, [Mbit/sec]
      > Tag: Operating Mode Notification
      > Tag: Power Capability Min: 8, Max: 20
      > Tag: Supported Channels
      > Tag: HT Capabilities (802.11n D1.10)
      > Tag: RSN Information
      > Tag: Mobility Domain
        Tag Number: Mobility Domain (54)
        Tag length: 3
        Mobility Domain Identifier: 0x34ac
      > FT Capability and Policy: 0x00
      > Tag: Supported Operating Classes
```



Over-The-DS

- + By default, new WLANs with 802.11r Fast Transition enabled operate as “FT Over the Air”
- + This means WLAN *clients must transmit their FT messages directly (over the air) to the new access point*
- + **Cisco recommends “FT Over the Air”**
- + 802.11r also supports WLAN clients sending FT messages over the Distribution System (DS) prior to roaming.
- + Allows WLAN clients and APs to utilize the wired Distribution System (and WLC) to forward FT messages.

Over-the-DS Configuration

Edit WLAN

⚠ Changing WLAN parameters while it is enabled will result in loss of connectivity for clients connected to it.

General **Security** Advanced Add To Policy Tags

Layer2 Layer3 AAA

WPA + WPA2 WPA2 + WPA3 WPA3 Static WEP None

MAC Filtering

Lobby Admin Access

WPA Parameters

WPA Policy WPA2 Policy

GTK Randomize OSEN Policy

WPA2 Encryption


AES(CCMP128) CCMP256

Fast Transition

Status Enabled

Over the DS

Reassociation Timeout * 20



FT with Over-the-Air

```
> IEEE 802.11 Beacon frame, Flags: .....C
v IEEE 802.11 Wireless Management
  > Fixed parameters (12 bytes)
  v Tagged parameters (290 bytes)
    > Tag: SSID parameter set: "Dot1x-Test"
    > Tag: Supported Rates 6(B), 9, 12(B), 18, 24(B), 36, 48, 54, [Mbit/sec]
    > Tag: DS Parameter set: Current Channel: 116
    > Tag: Traffic Indication Map (TIM): DTIM 0 of 1 bitmap
    > Tag: Country Information: Country Code US, Environment All
    > Tag: Power Constraint: 0
    > Tag: RSN Information
    > Tag: OBSS Load Element 802.11e CCA Version
  v Tag: Mobility Domain
    Tag Number: Mobility Domain (54)
    Tag length: 3
    Mobility Domain Identifier: 0x34ac
  v FT Capability and Policy: 0x00
    .... 0 = Fast BSS Transition over DS: 0x0
    .... ..0. = Resource Request Protocol Capability: 0x0
    0000 00.. = Reserved: 0x00
```

Over-the-DS Verification

```

v Tag: Mobility Domain
  Tag Number: Mobility Domain (54)
  Tag length: 3
  Mobility Domain Identifier: 0x34ac
v FT Capability and Policy: 0x01
  .... ...1 = Fast BSS Transition over DS: 0x1 ←
  .... ..0. = Resource Request Protocol Capability: 0x0
  0000 00.. = Reserved: 0x00
```

When to use Over-The-DS?

- + Over the DS can be useful in Congested RF Conditions
 - + The client remains on its current channel
 - + Client maintains data flow
 - + Client avoids extra delays that come from switching channels during scanning or handoff
- + **Caveats to Consider**
 - + Over-the-DS may suffer delays due to hair-pinning through the controller rather than direct AP-to-AP communication
 - + Over-the-DS works best **only when the DS path (WLC and wired network) is very low-latency and uncongested.**



**Thank you for
watching!!**

Getting There with Wireless Mobility & Roaming - Summary

<https://t.me/learningnets>



Key Concepts - Recap

- + Roaming Fundamentals & Categories
- + Mobility Groups & Tunneling
- + Layer-3 Inter-Controller Roaming
- + Optimizing Roaming Performance



Learning Outcomes Recap

- + Explain wireless roaming concepts
- + Describe mobility groups and mobility tunnels
- + Identify roaming triggers and latency factors
- + Configure and verify fast secure roaming techniques
- + Monitor and troubleshoot roaming events
- + Summarize the roaming workflow

Next Steps

- + Purchase your own access points and practice concepts you learned in the course.
- + Dive deeper into learning about 802.1x for WLANs
- + Review all INE courses in the Learning Path, “Wireless Enterprise Networking”

THANKS FOR WATCHING!

<https://t.me/learningnets>



EXPERTS AT MAKING YOU AN EXPERT

