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

PREREQUISITES

- 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

LET'S GO!

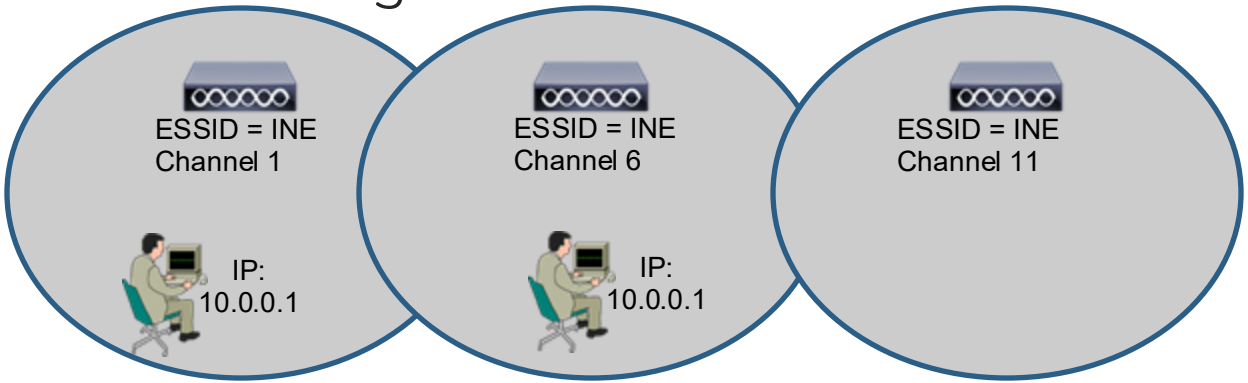
What is Roaming?

What is Wireless Roaming?

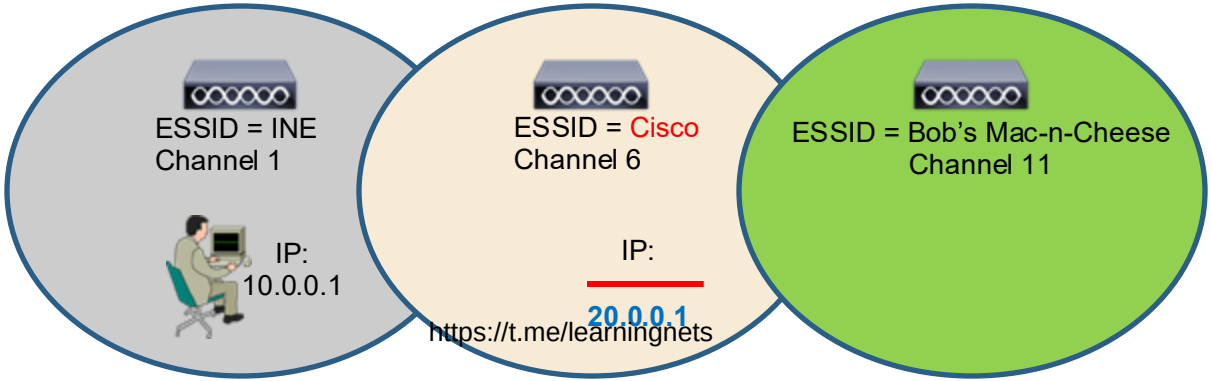
- Roaming is the process where a wireless client device transitions its connection from one AP to another without losing network connectivity.
- Wireless client must maintain its IPv4/IPv6 address in order to qualify as a roaming event.

Roaming Defined

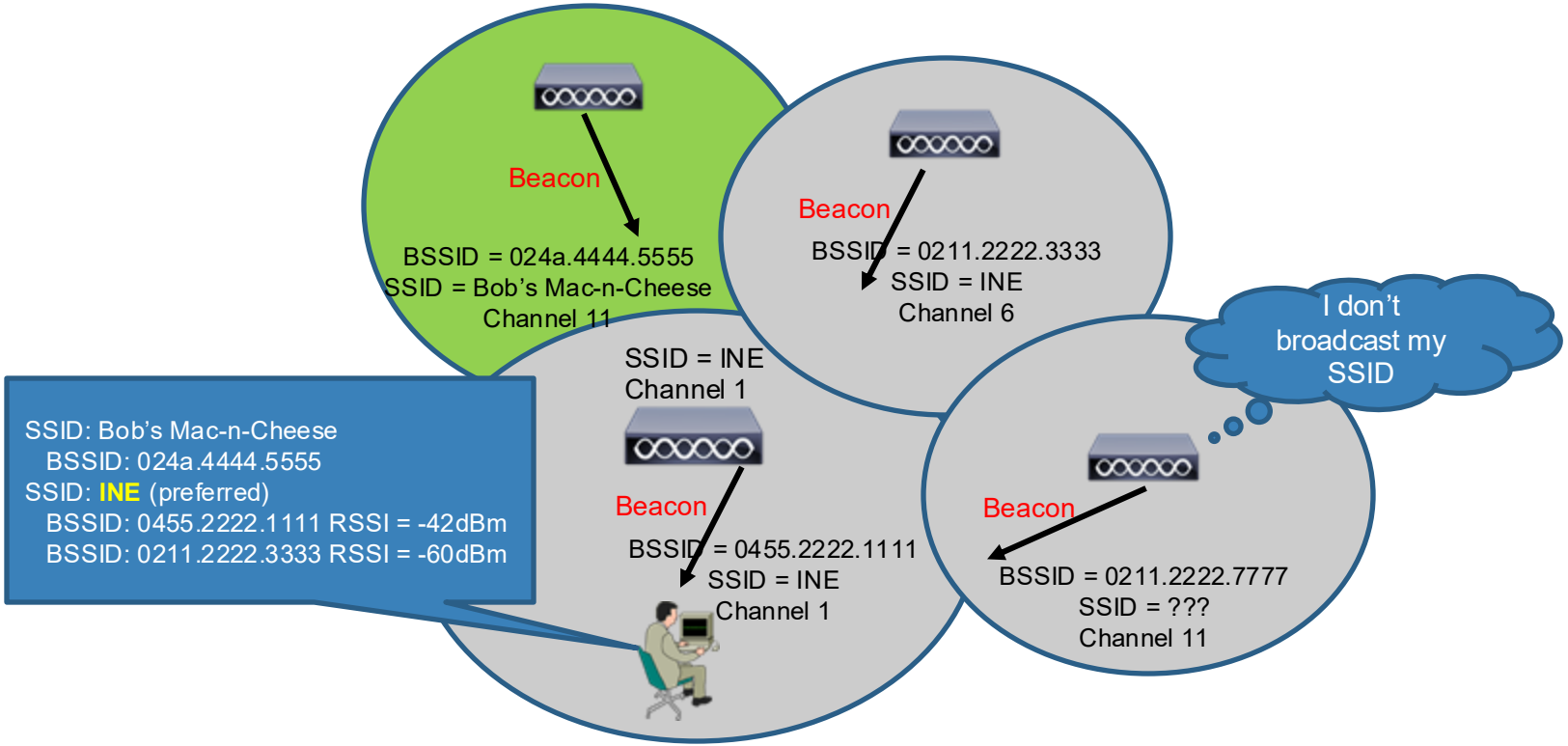
- What roaming IS



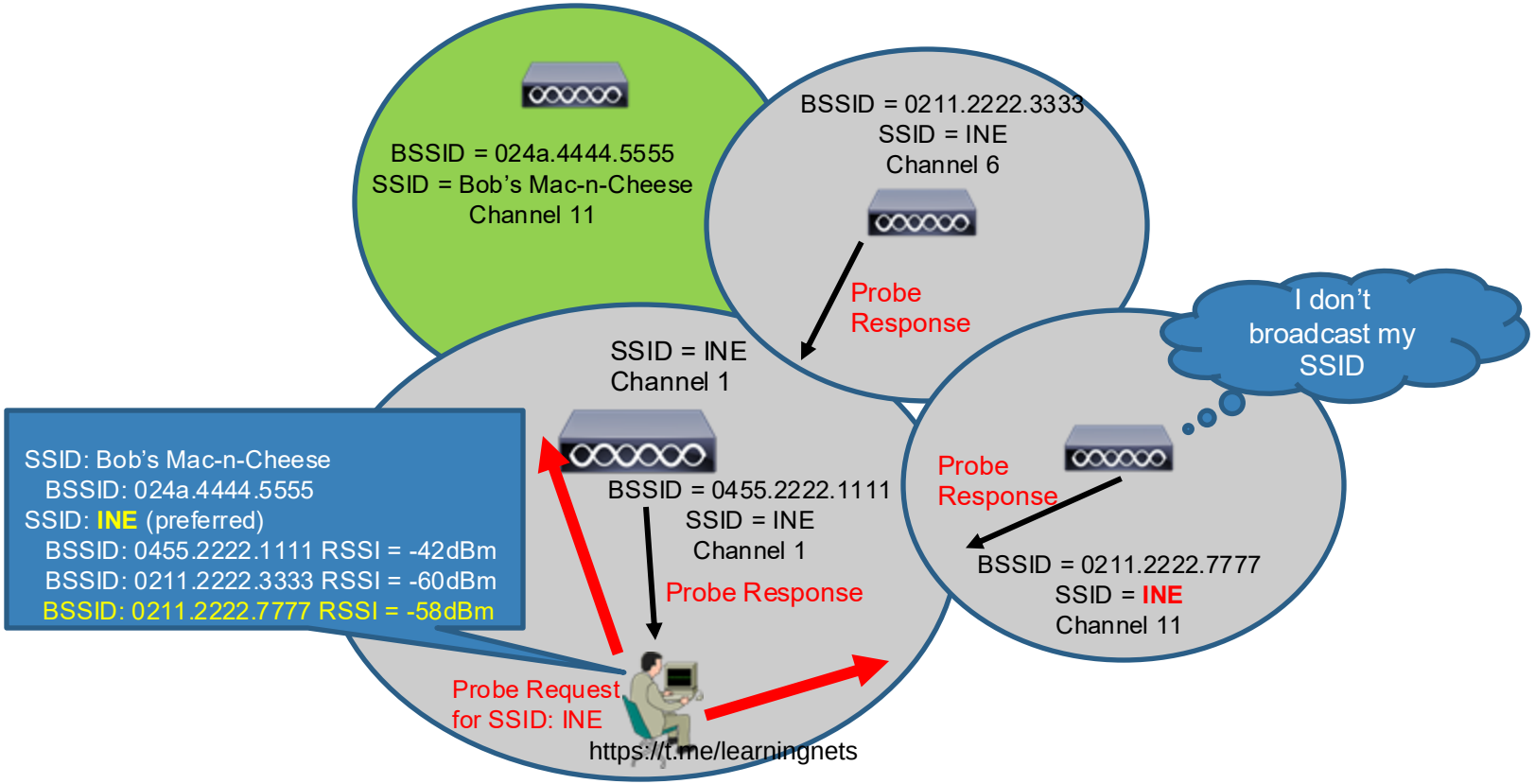
- What roaming ISN'T



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

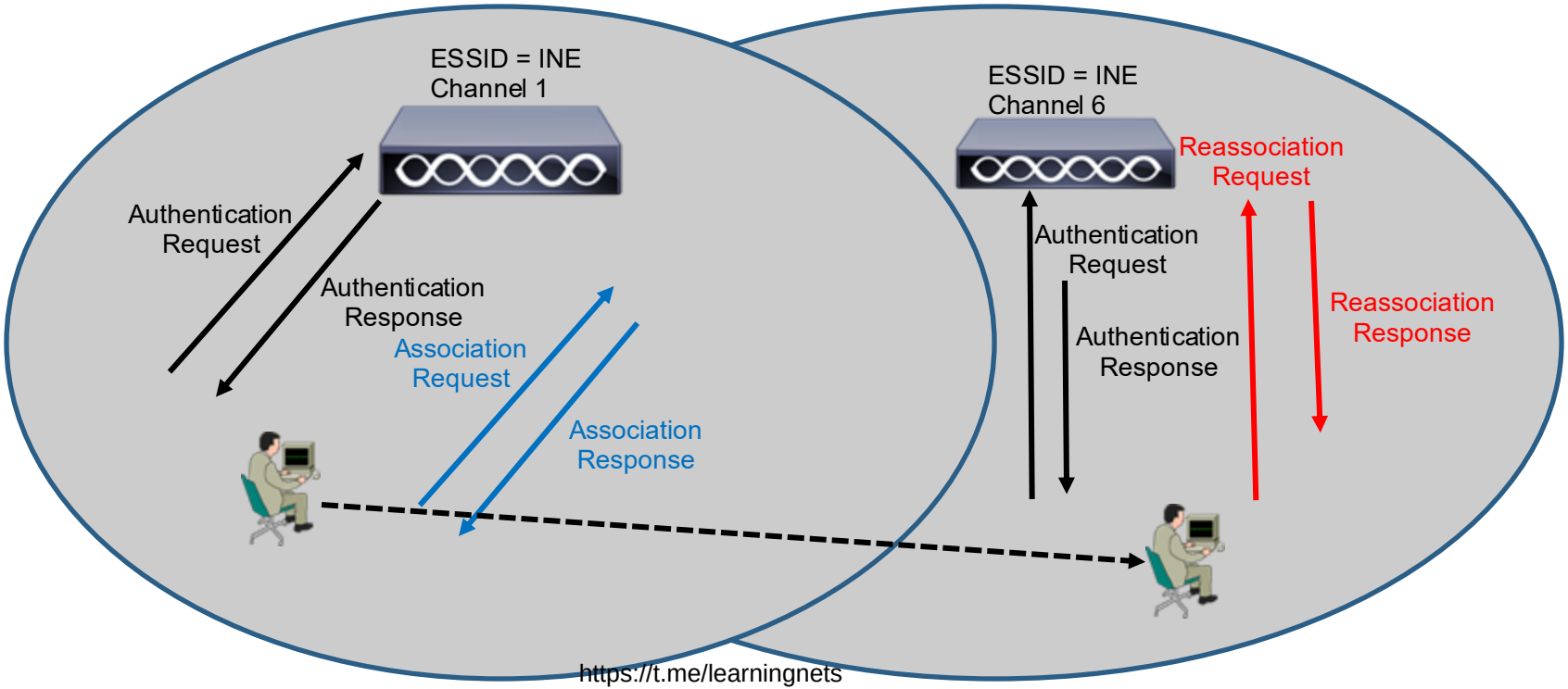
Client Proprietary Algorithms

- 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).

https://community.intel.com/t5/Wireless/Roaming-aggressiveness-and-Signal-strength/m-p/462734

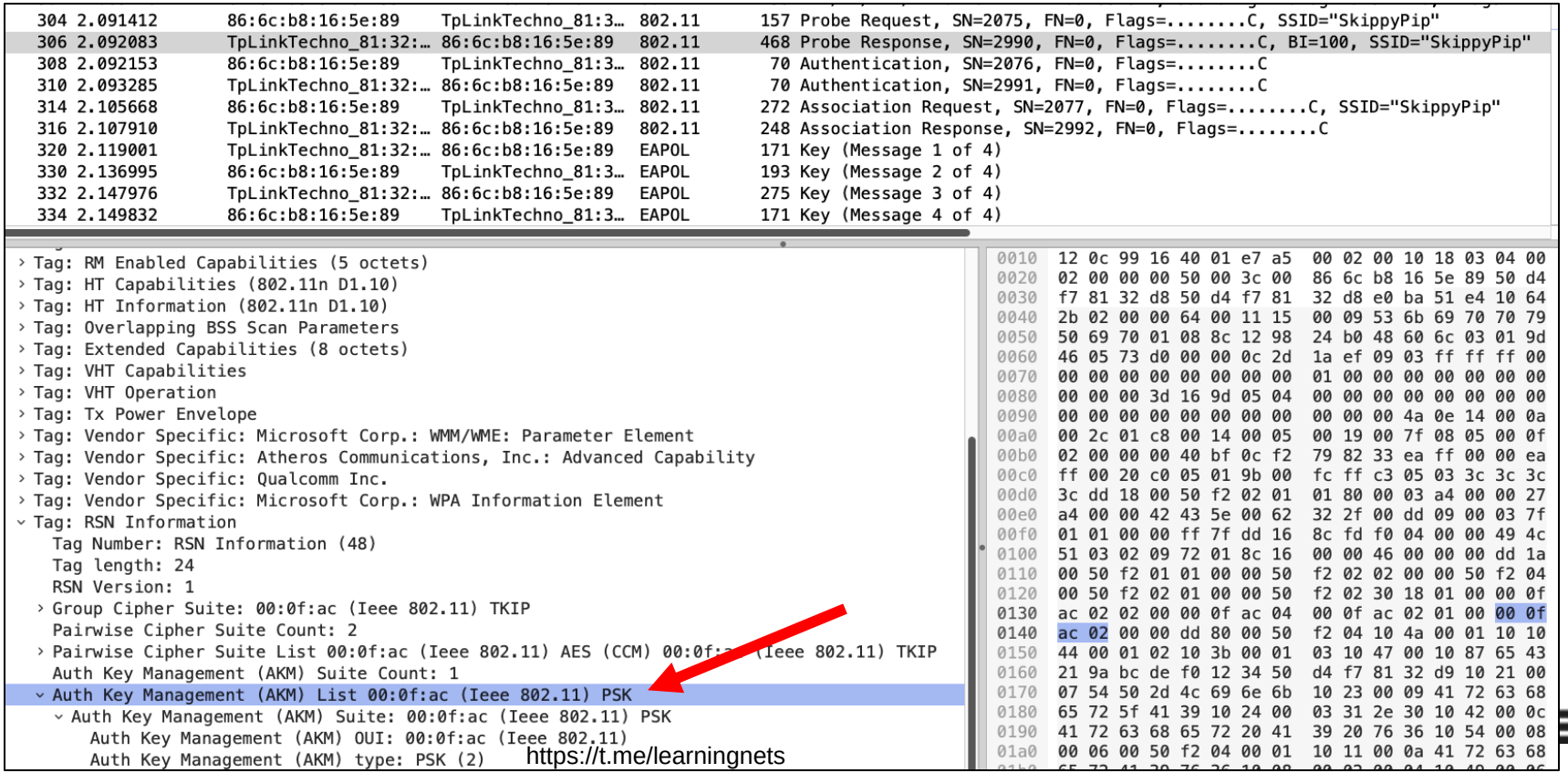
Association & Reassociation



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



Thank you for watching!!

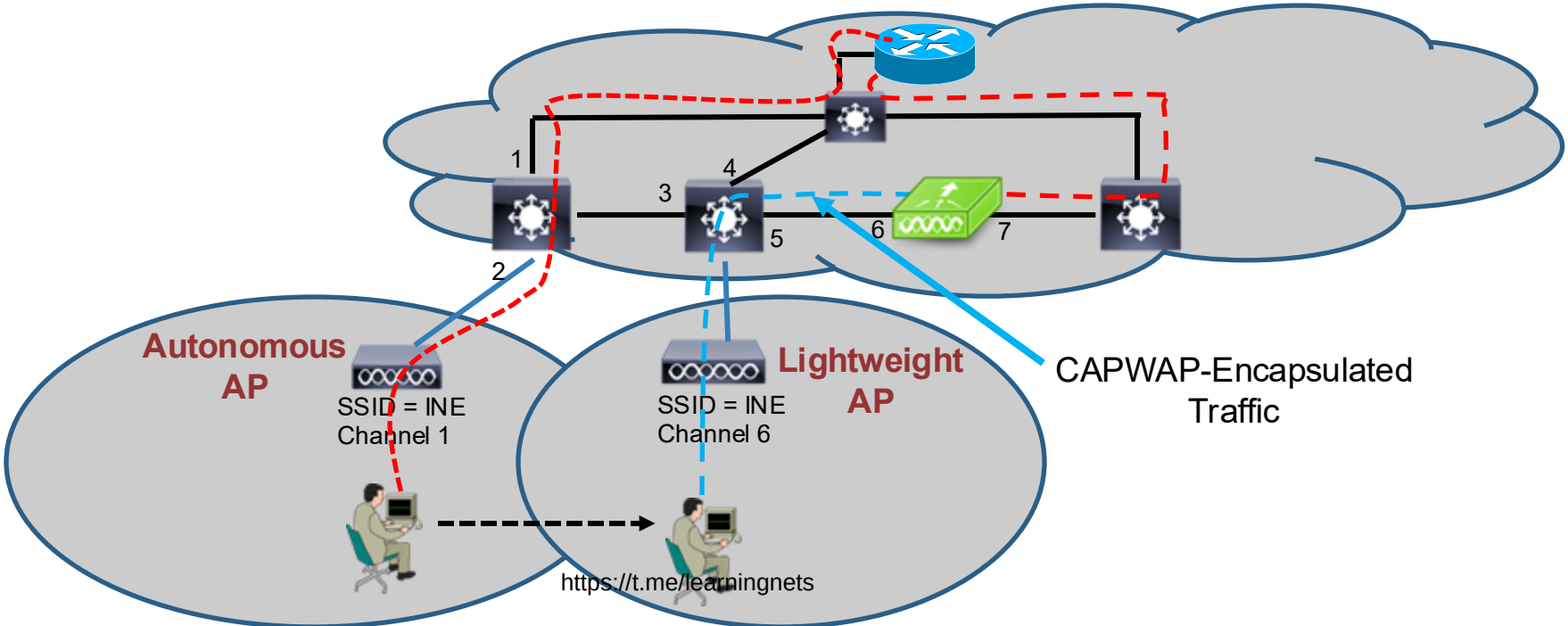
Categories of Wireless Roaming

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.

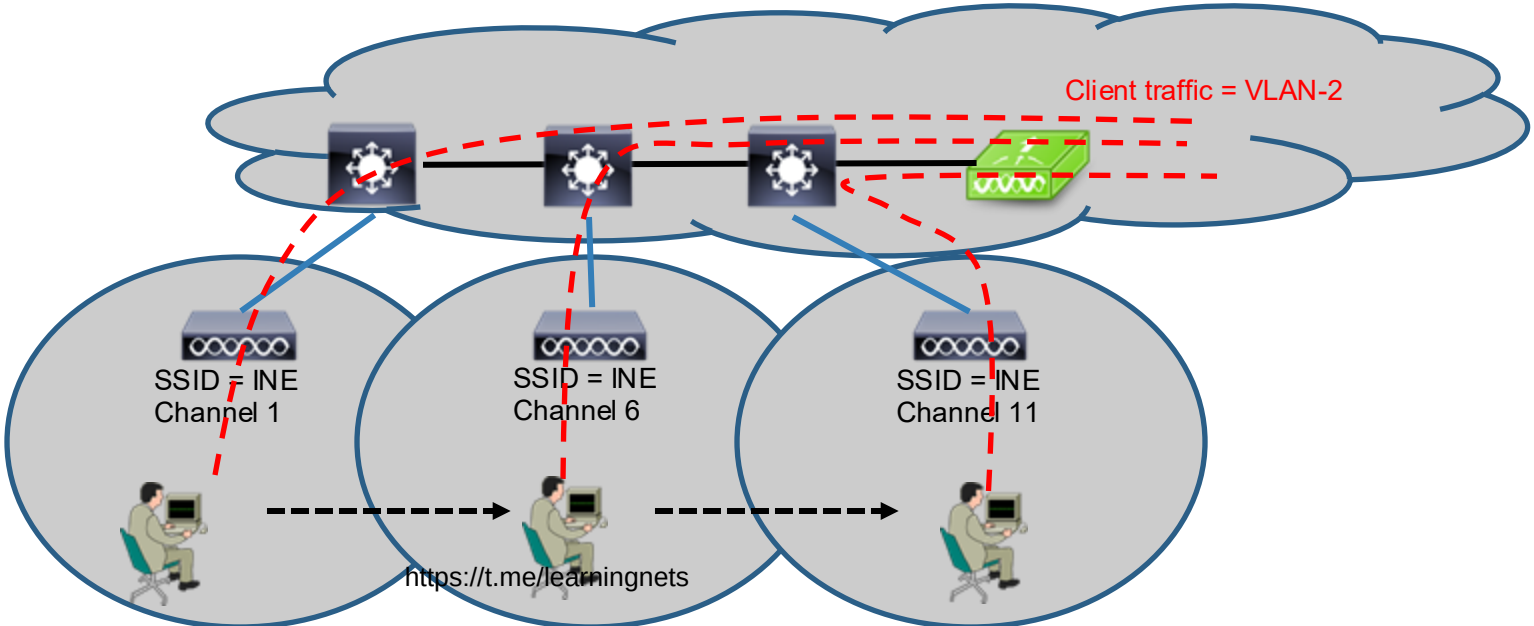
Autonomous Roam

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



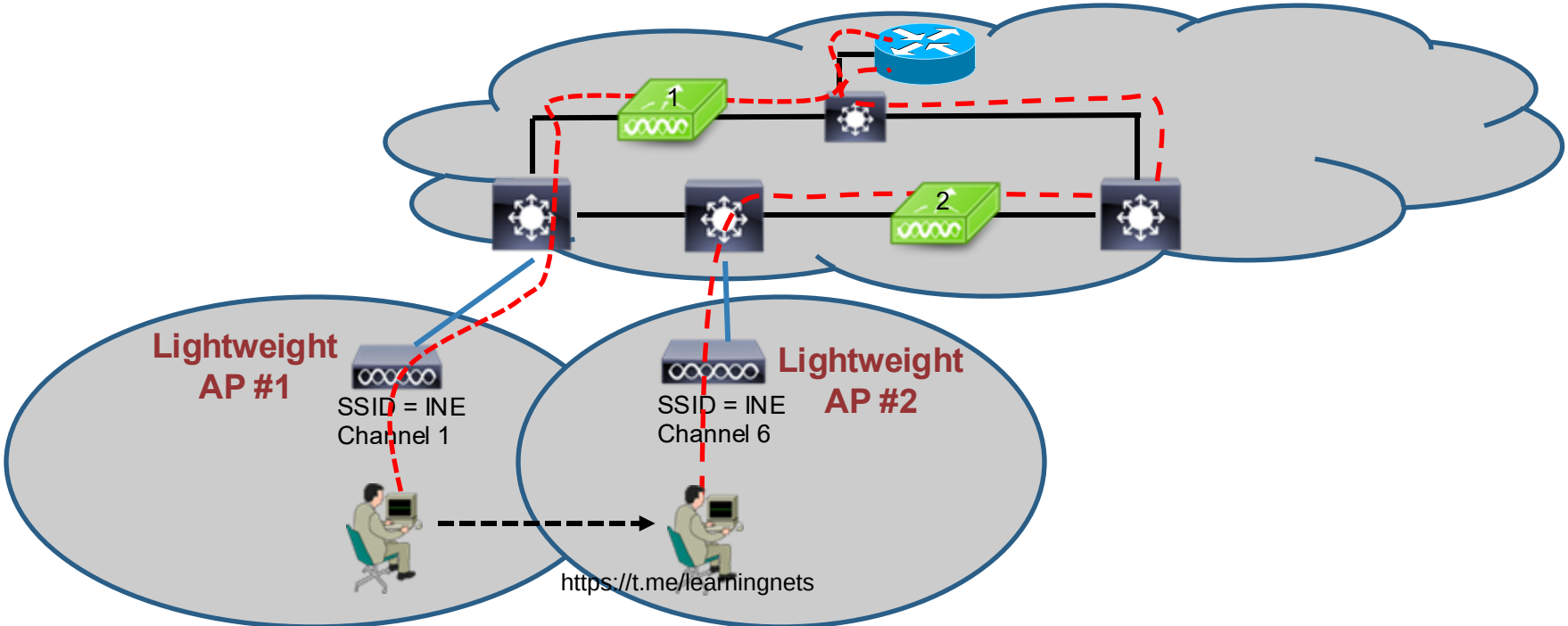
Intra-Controller Roam

- 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

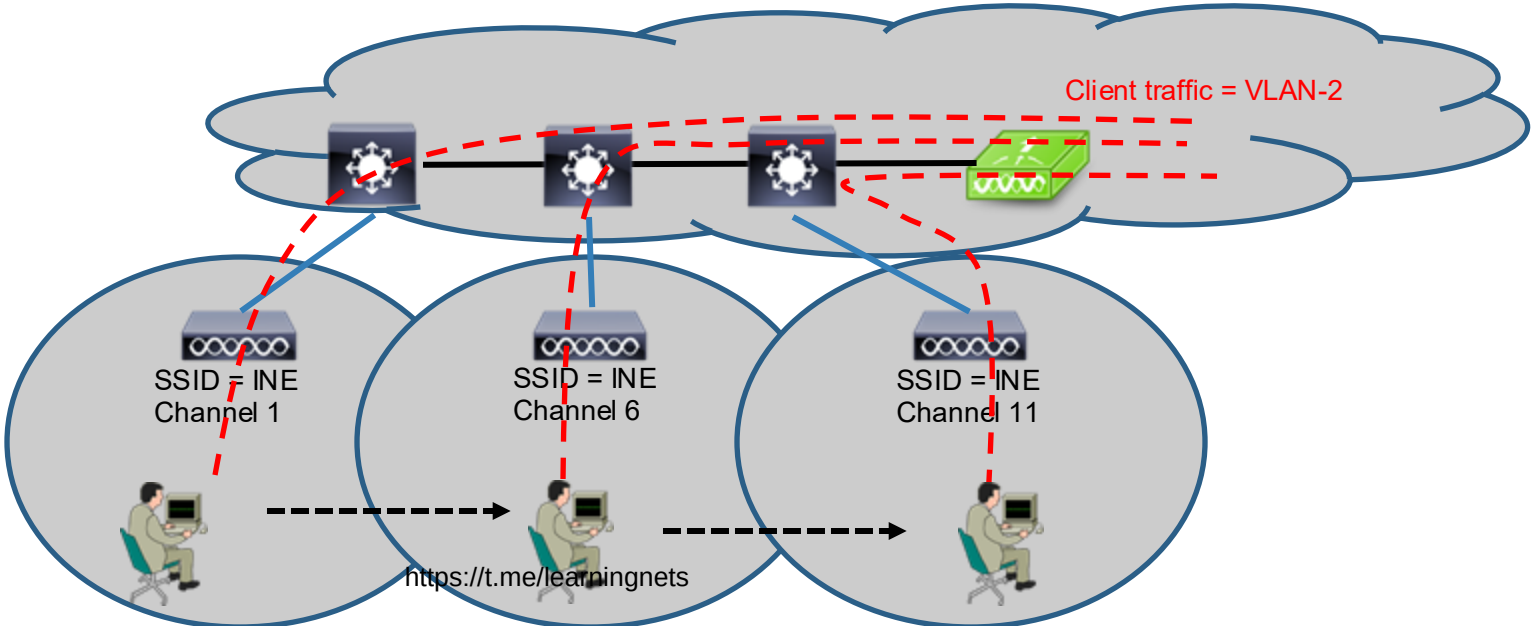


Layer-2 or Layer-3?

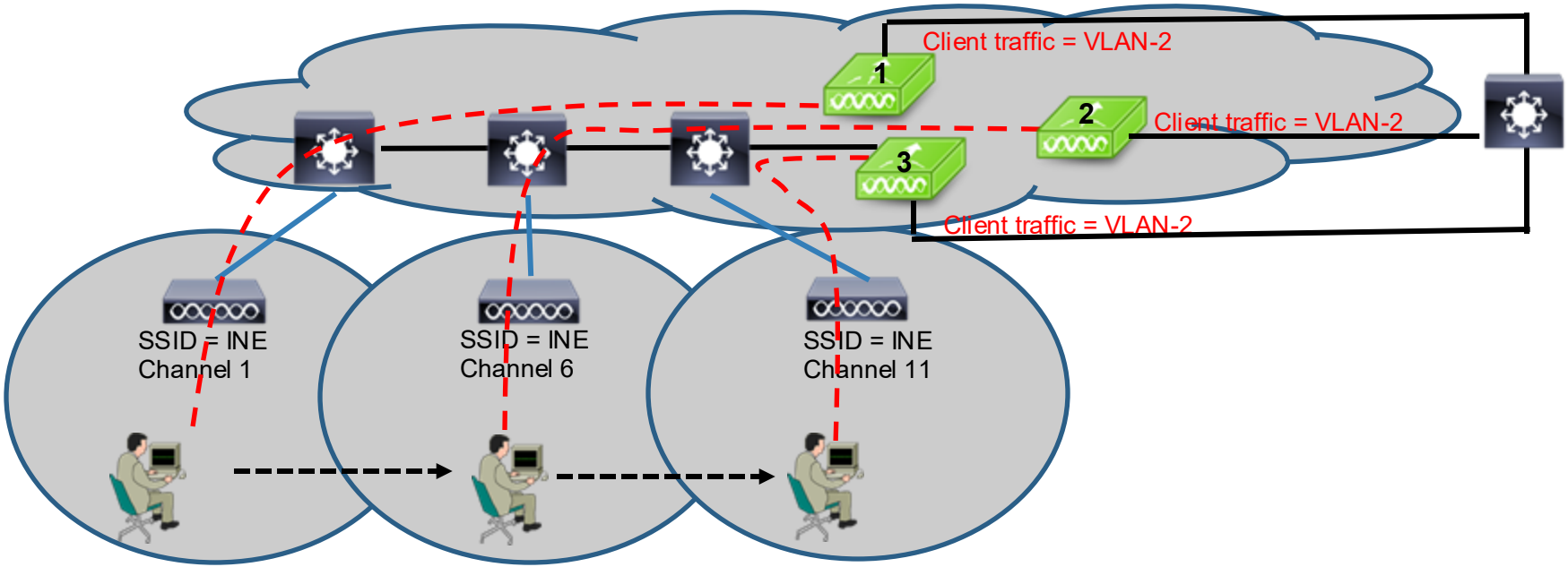
- Inter-Controller roaming is also defined as either:
  - Layer-2 roaming
  - Layer-3 roaming
- The controller's uplink mapping of SSID-to-VLAN is what makes the difference
  - Two controllers, same SSID, same VLAN-to-SSID mapping = Layer-2 roam
  - Two controllers, same SSID, different VLAN-to-SSID 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

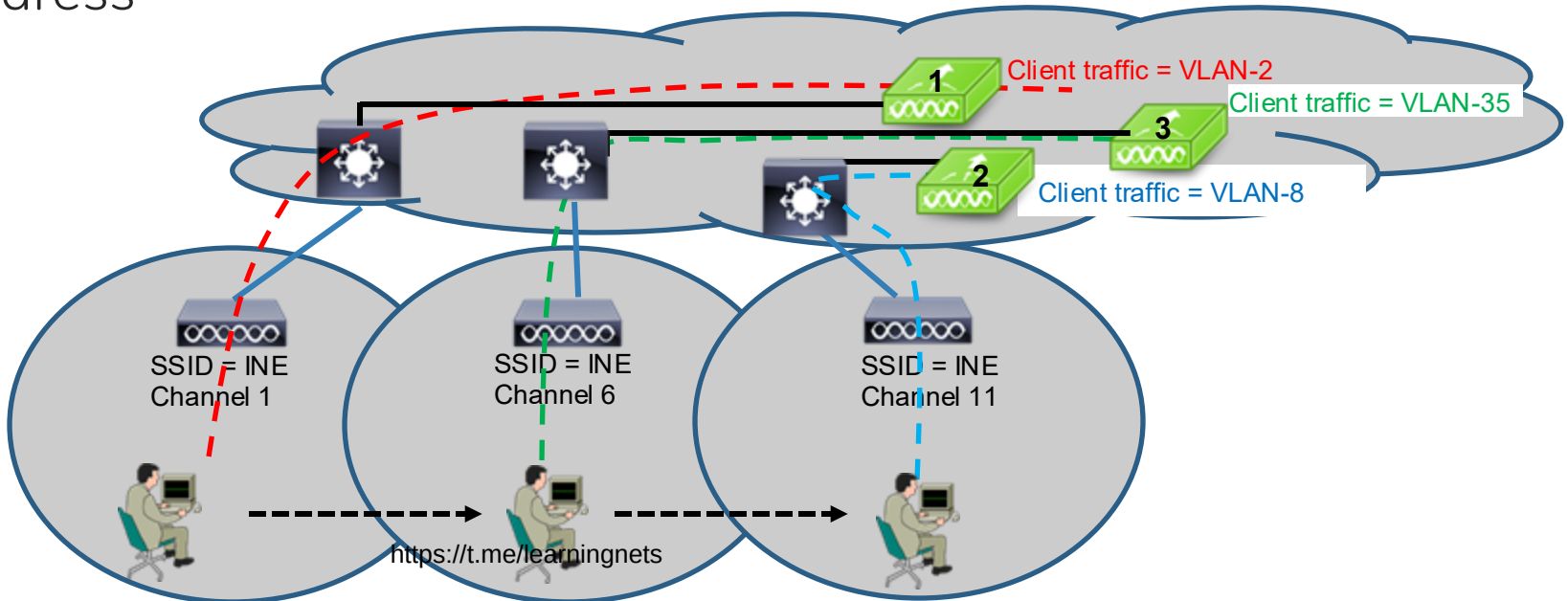


Layer-2 Roaming (Inter-Controller)



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

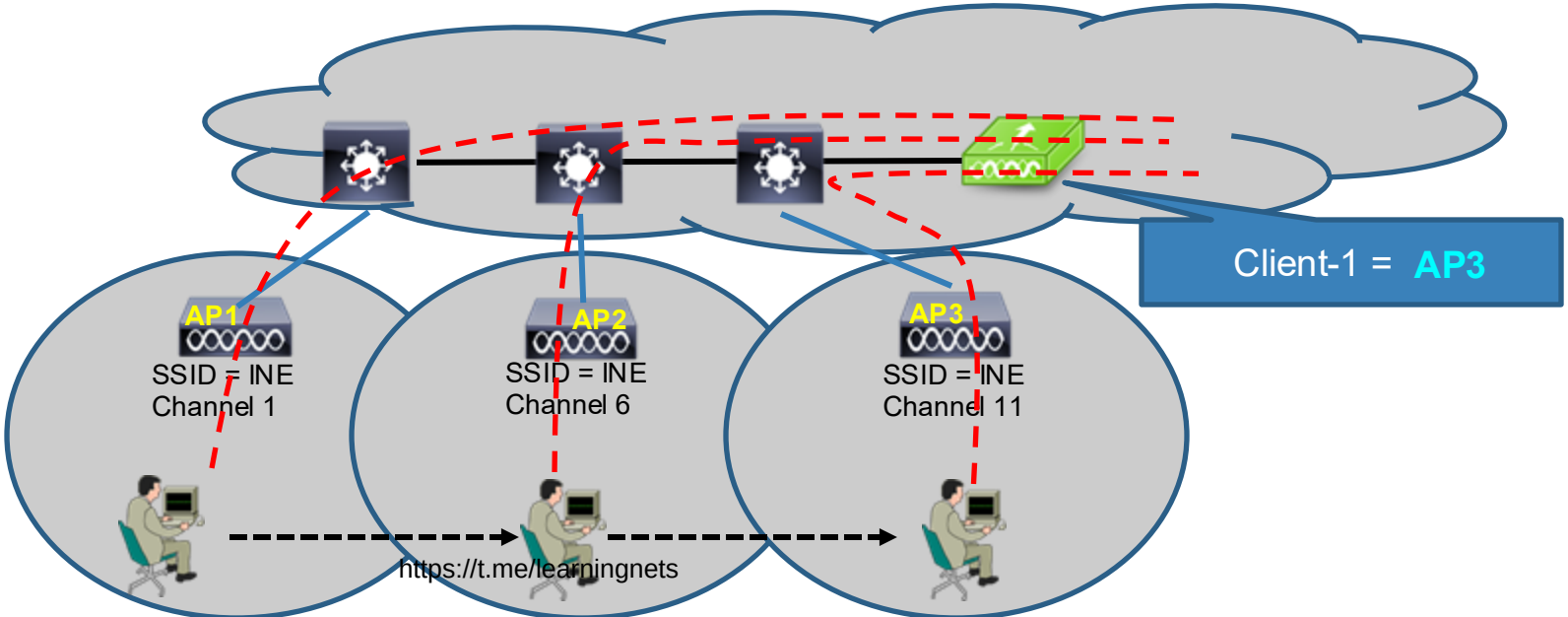


Thank you for watching!!

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

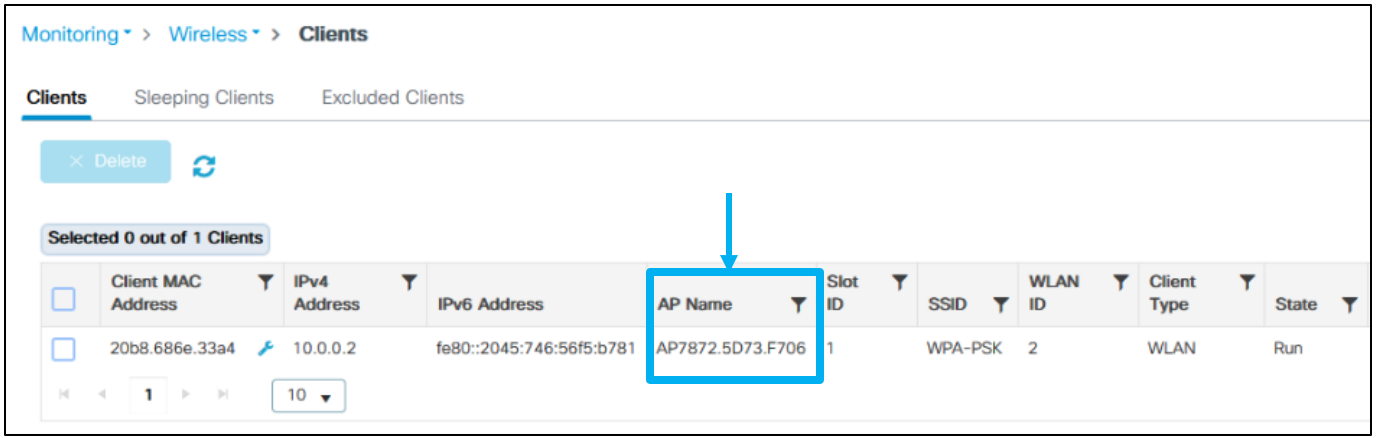


Controller Client Entries

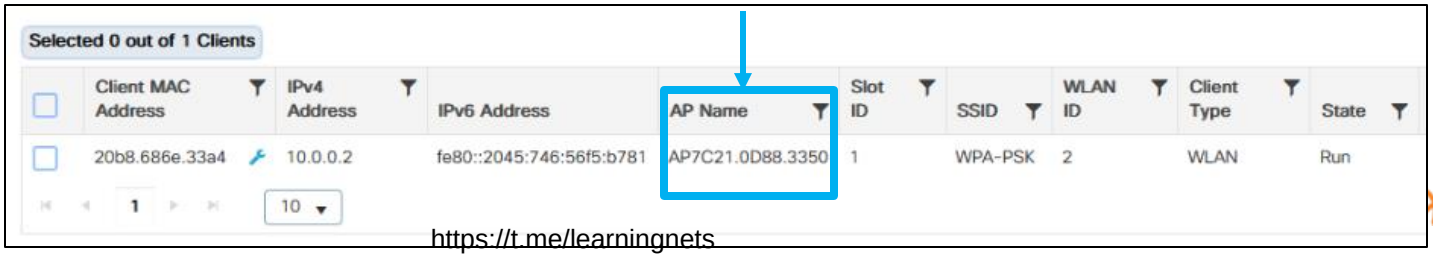
- When a wireless client associates/authenticates to an access point, the controller creates a client database entry
- Entry includes:
  - Client's MAC and IP addresses
  - Security context and associations
  - Quality of Service (QoS) contexts
  - WLAN ID and associated access point
- Controller uses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

Viewing Client Information

- Before the roam…



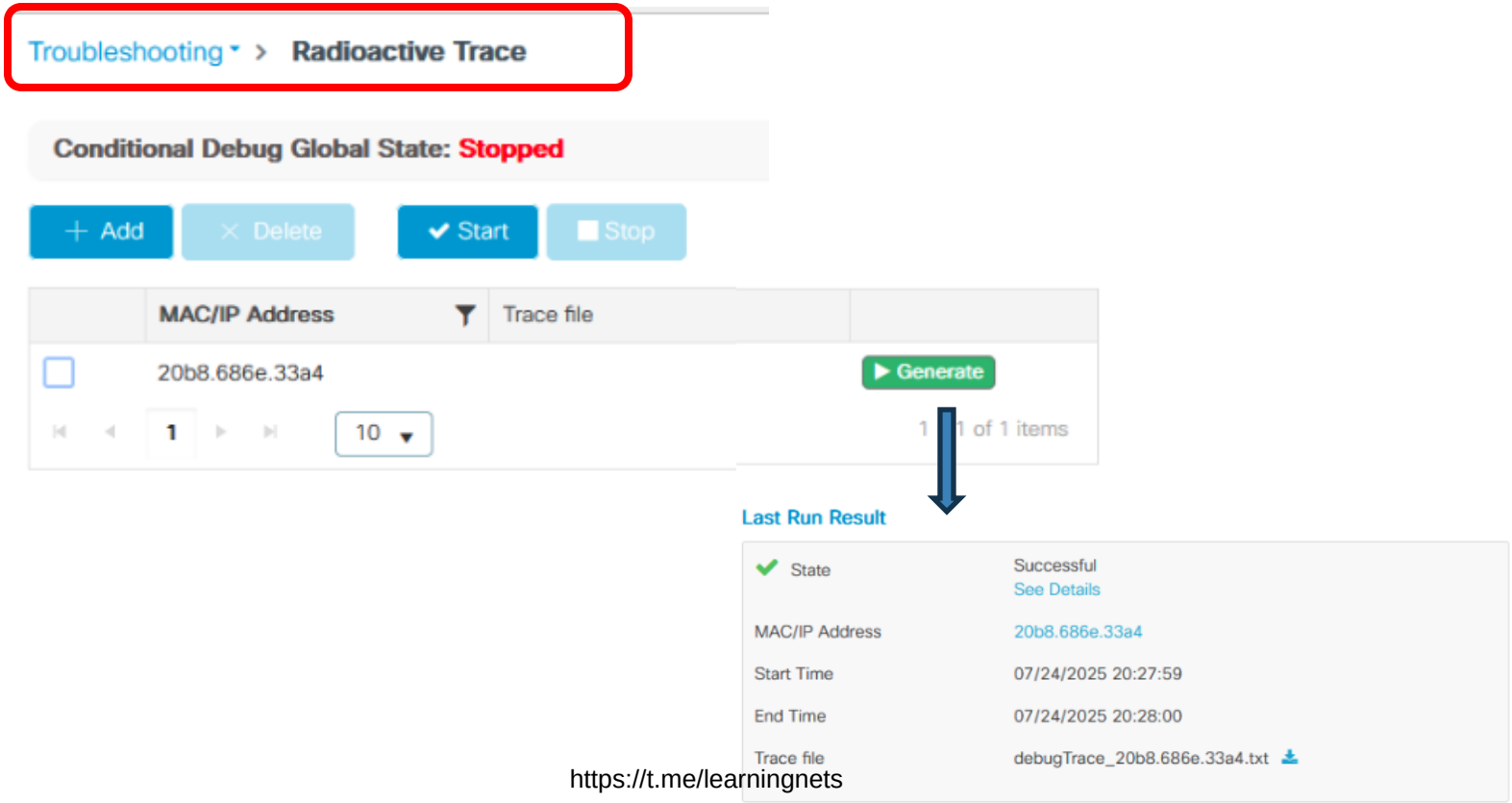
- After the roam…



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



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

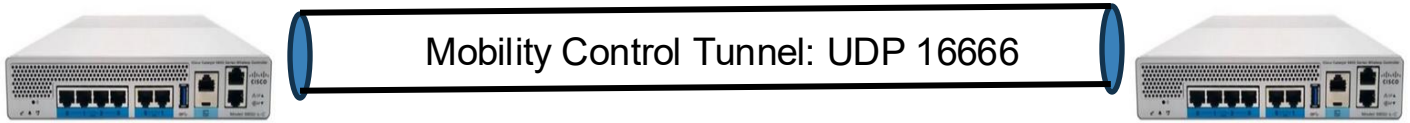
What are Mobility Groups?

- 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

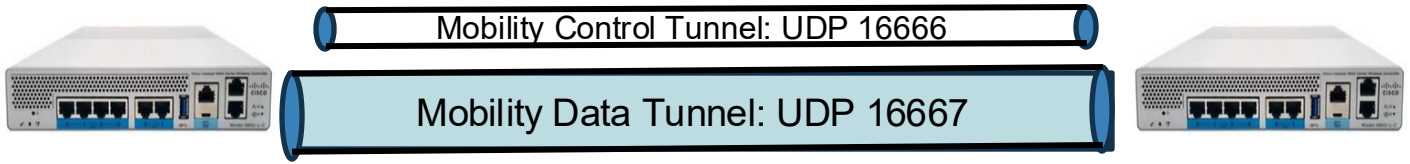
- Mobility peering creates UDP-based mobility tunnels between peers:
  - Mobility Control Tunnel
    - UDP port 16666
    - Implements DTLS encryption
  - Mobility Data Tunnel
    - UDP port 16667
    - Can be optionally configured for DTLS encryption

Mobility Control Tunnels



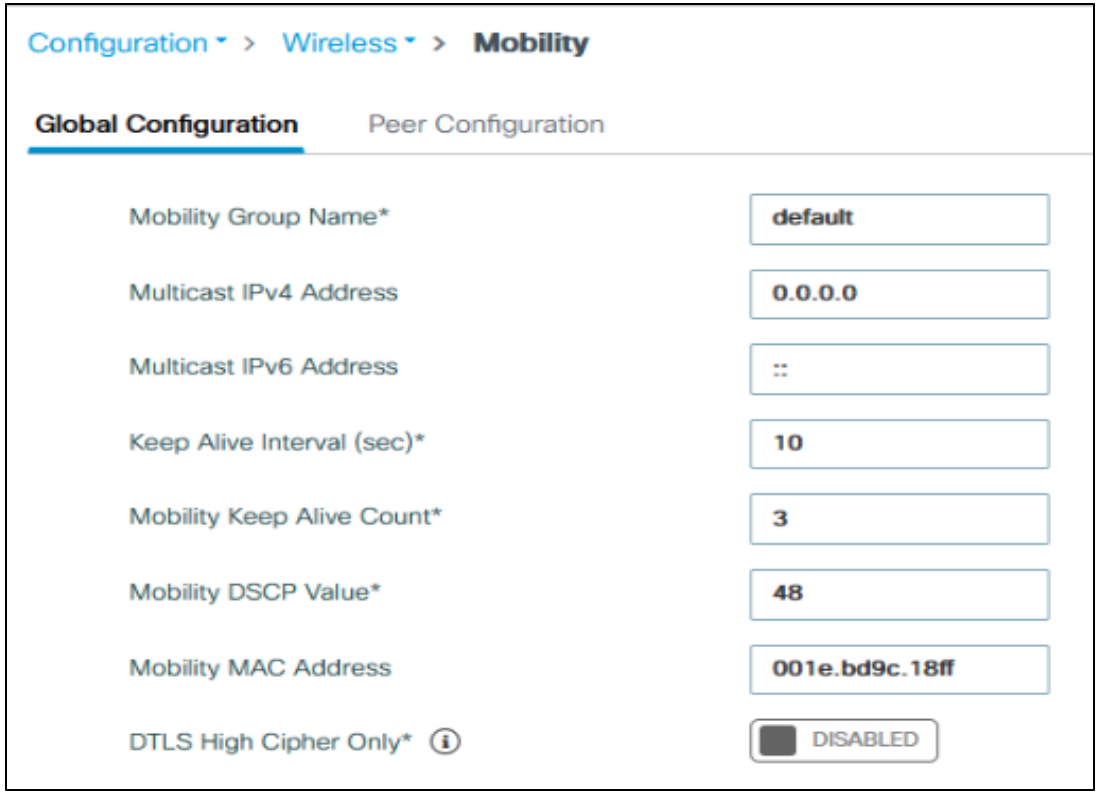
- Mobility Control Messages
- Heartbeats
- Client Session Synchronization
- Messages for optional fast roaming techniques
  - Fast Transition (FT) Control Messages
  - OKC (Opportunistic Key Caching) Control Messages

Mobility Data Tunnels



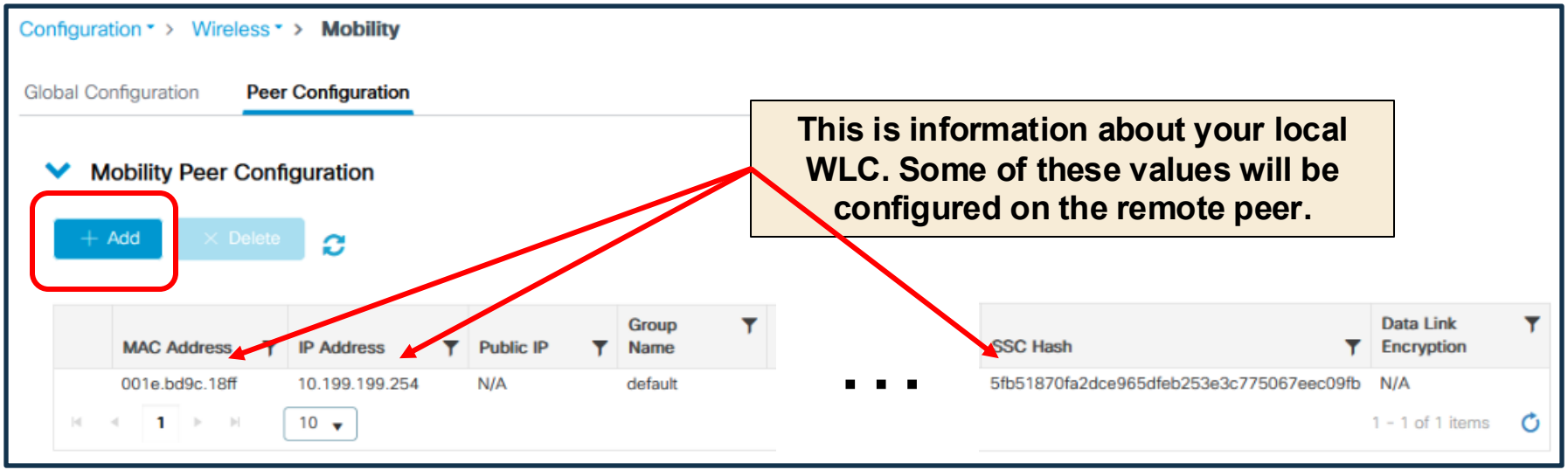
- Client data frames during Layer-3 roams
- Fast Transition (FT) pre-authentication data PDUs
- Diagnostic/Monitoring traffic
- Keepalive Packets: Periodic small packets to ensure the tunnel remains operational.

Mobility Global Configuration

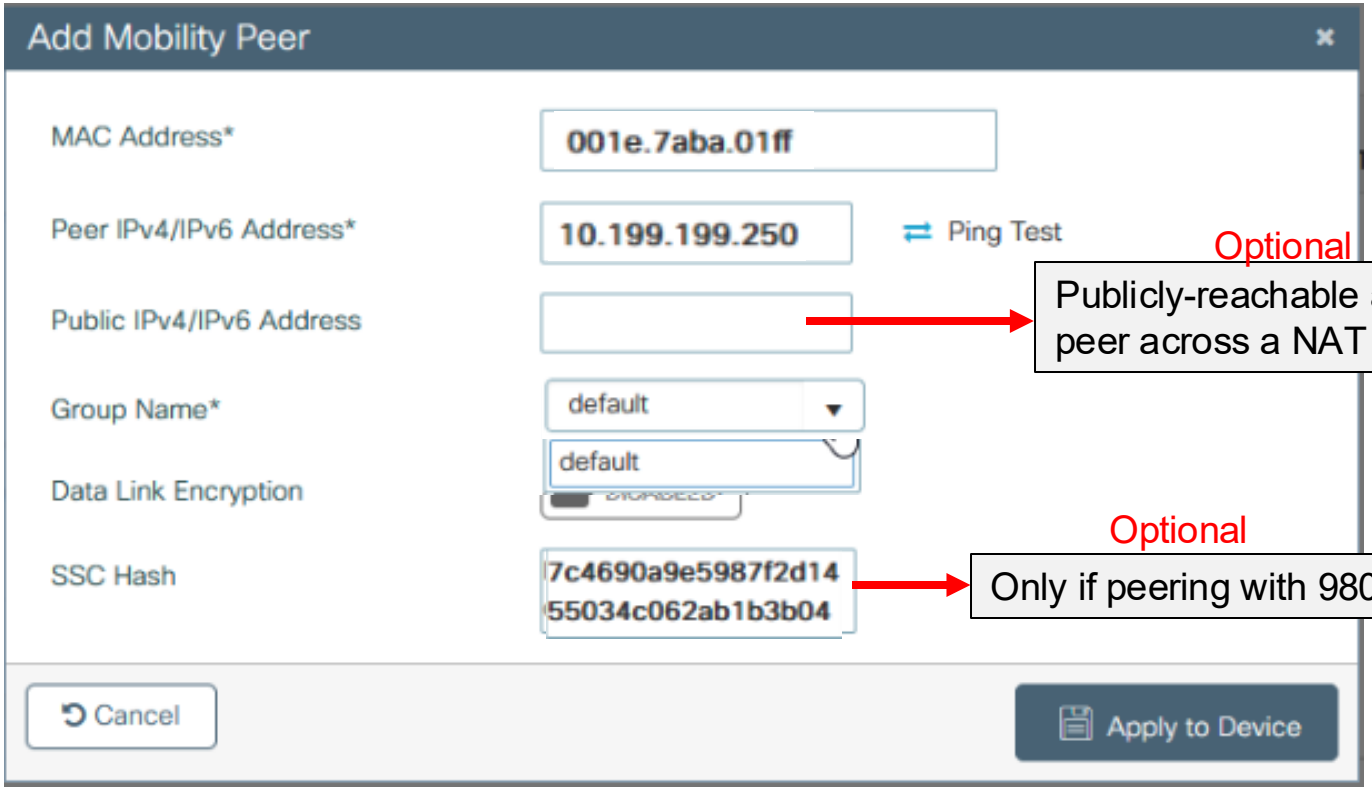


There is no need to change any of these values.

Mobility Peer Configuration (1)



Mobility Peer Configuration (2)



Mobility Peer Verification

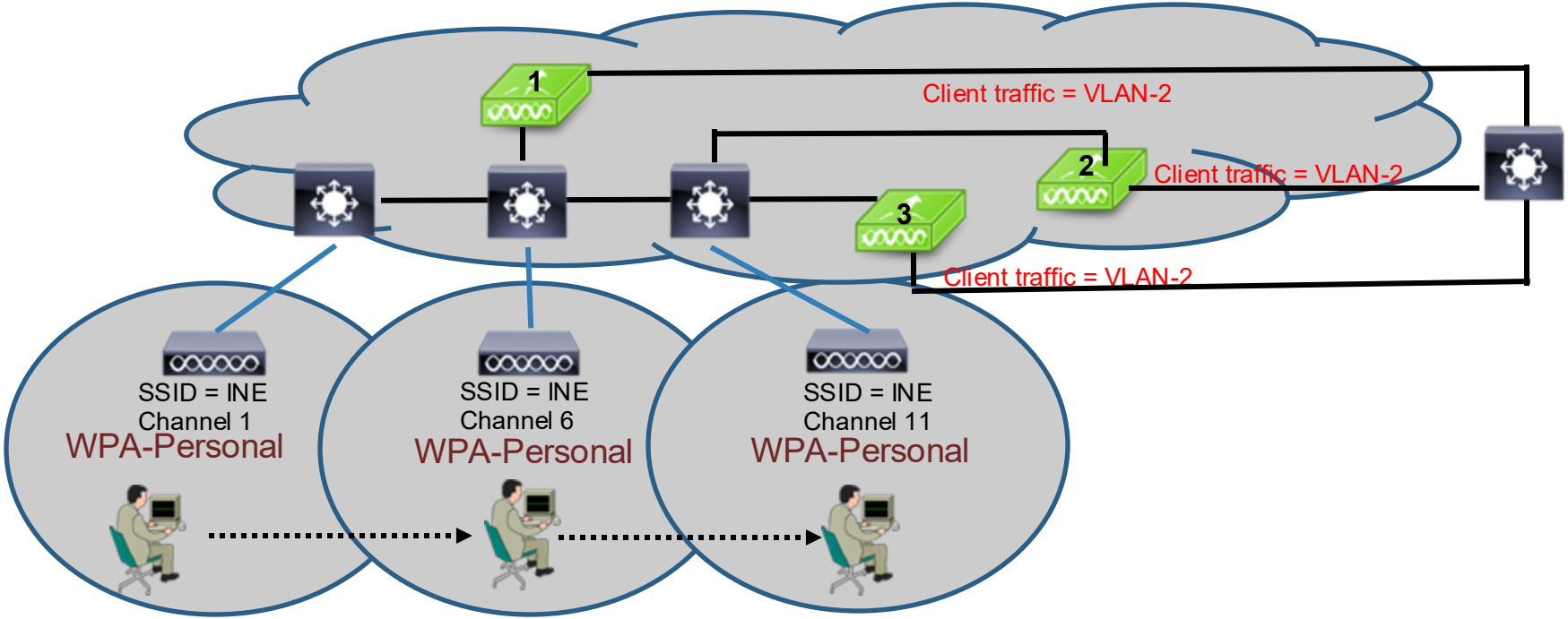
Thank you for watching!!

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…

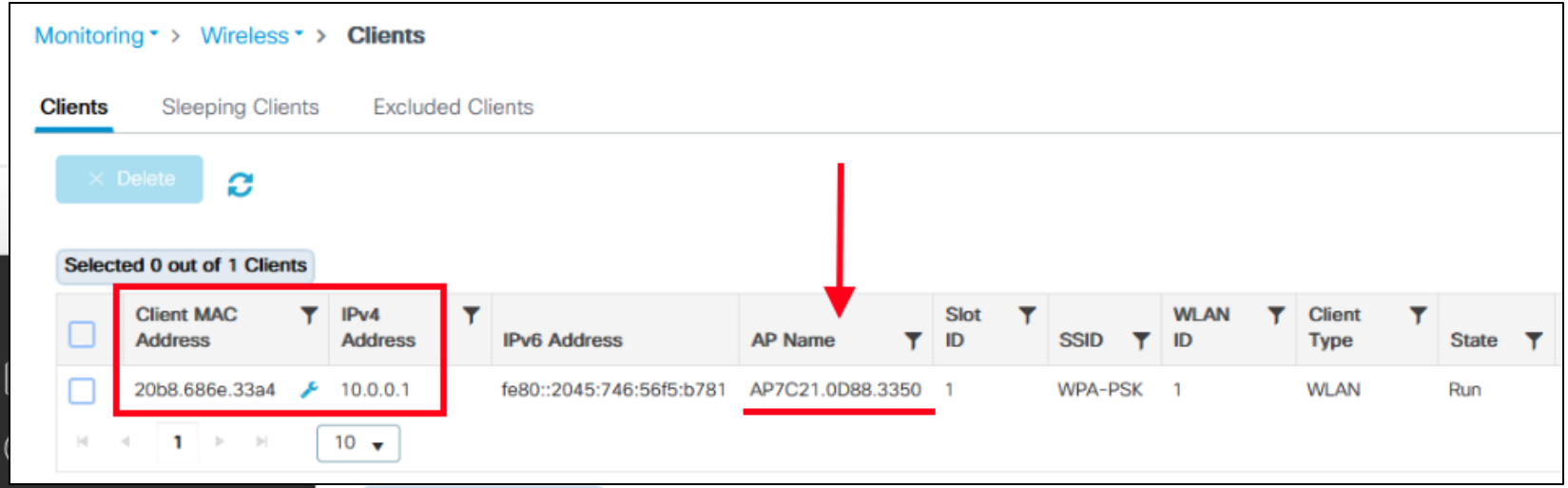
No Mobility Needed



PSK Inter-Controller Roam

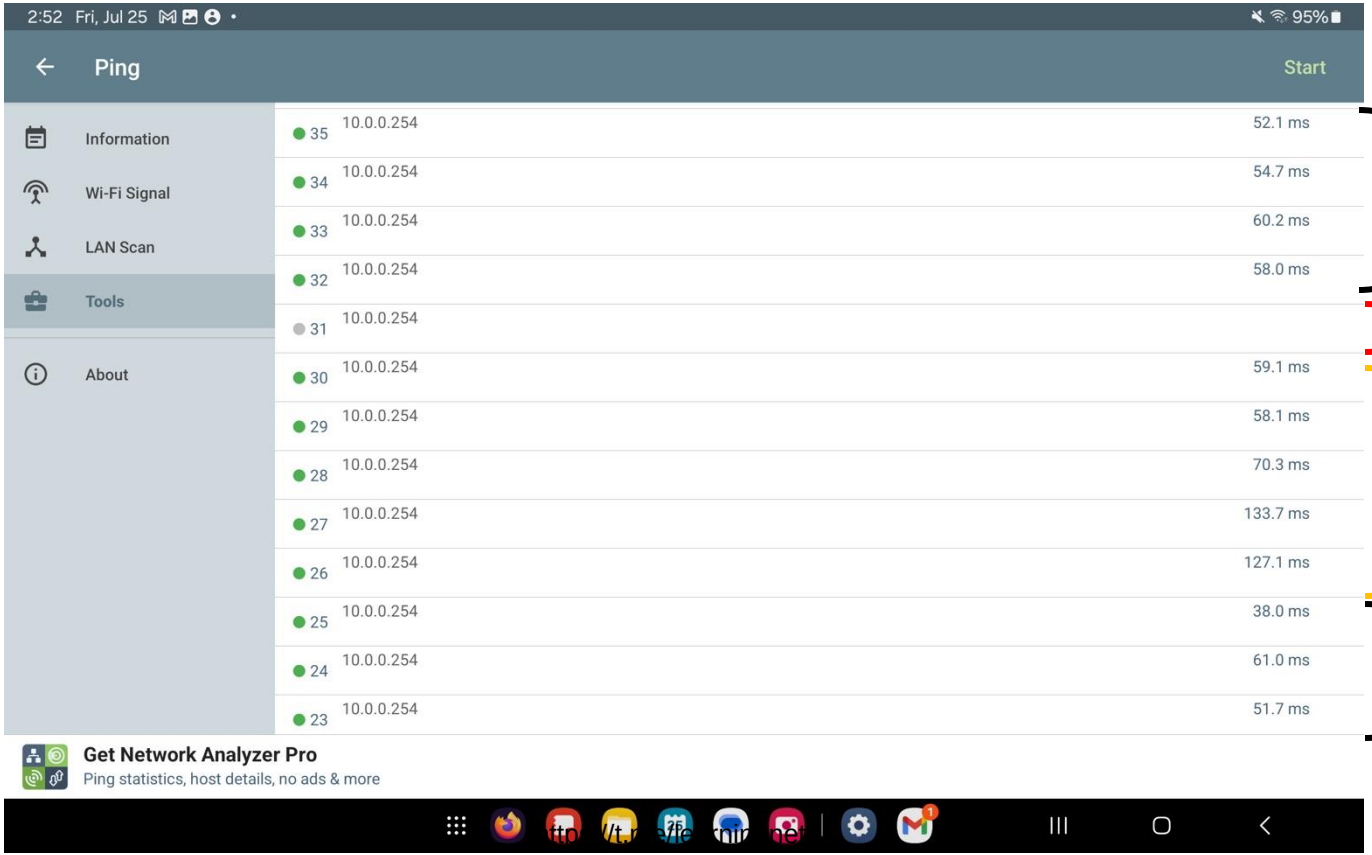
- No mobility groups have been configured

Post-Roam
(on 9800-2)



Pre-Roam
(on 9800-1)

PSK Inter-Controller Roam



Connected to AP-2

PSK Re-Authentication

Equidistant between AP-1 and AP-2 (DRS??)

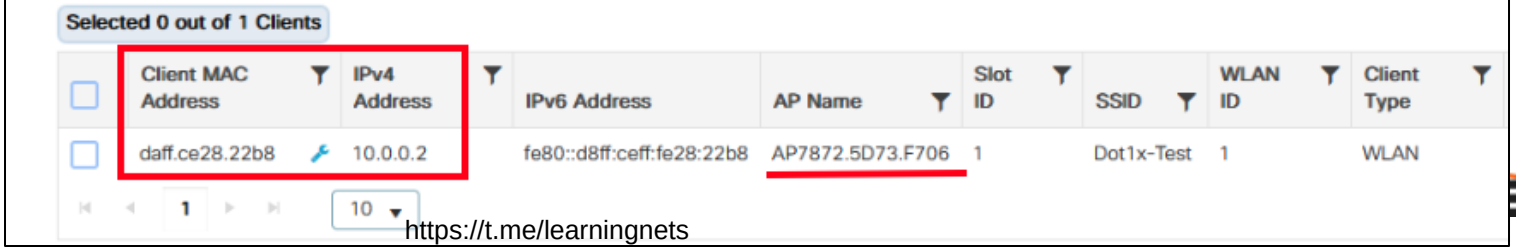
Connected to AP-1 (avg = 53.56 ms)

802.1x Inter-Controller Roam

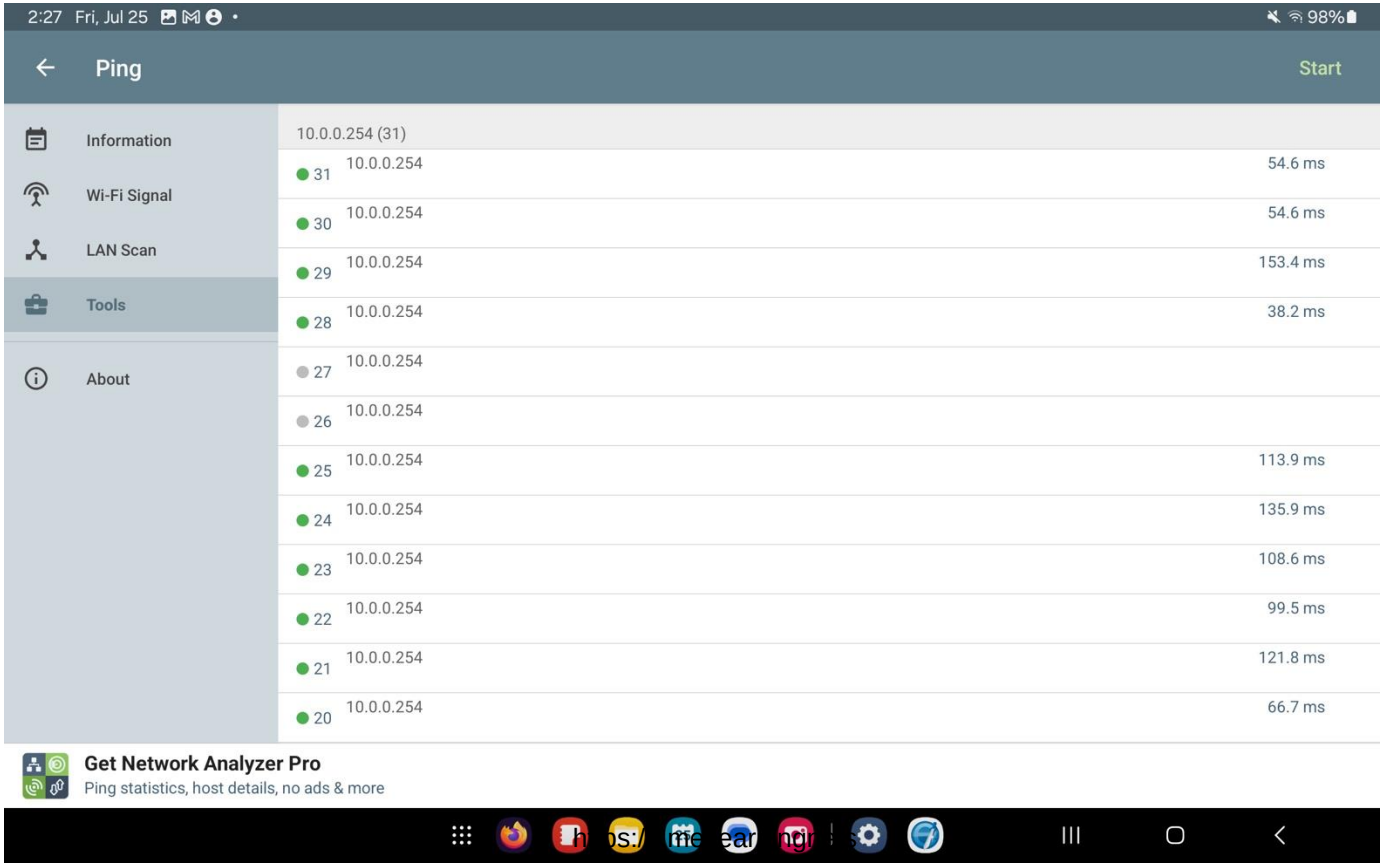
- No Mobility Groups have been configured

Post-Roam
9800-2

Pre-Roam
9800-1



802.1x Data Loss without Mobility Group



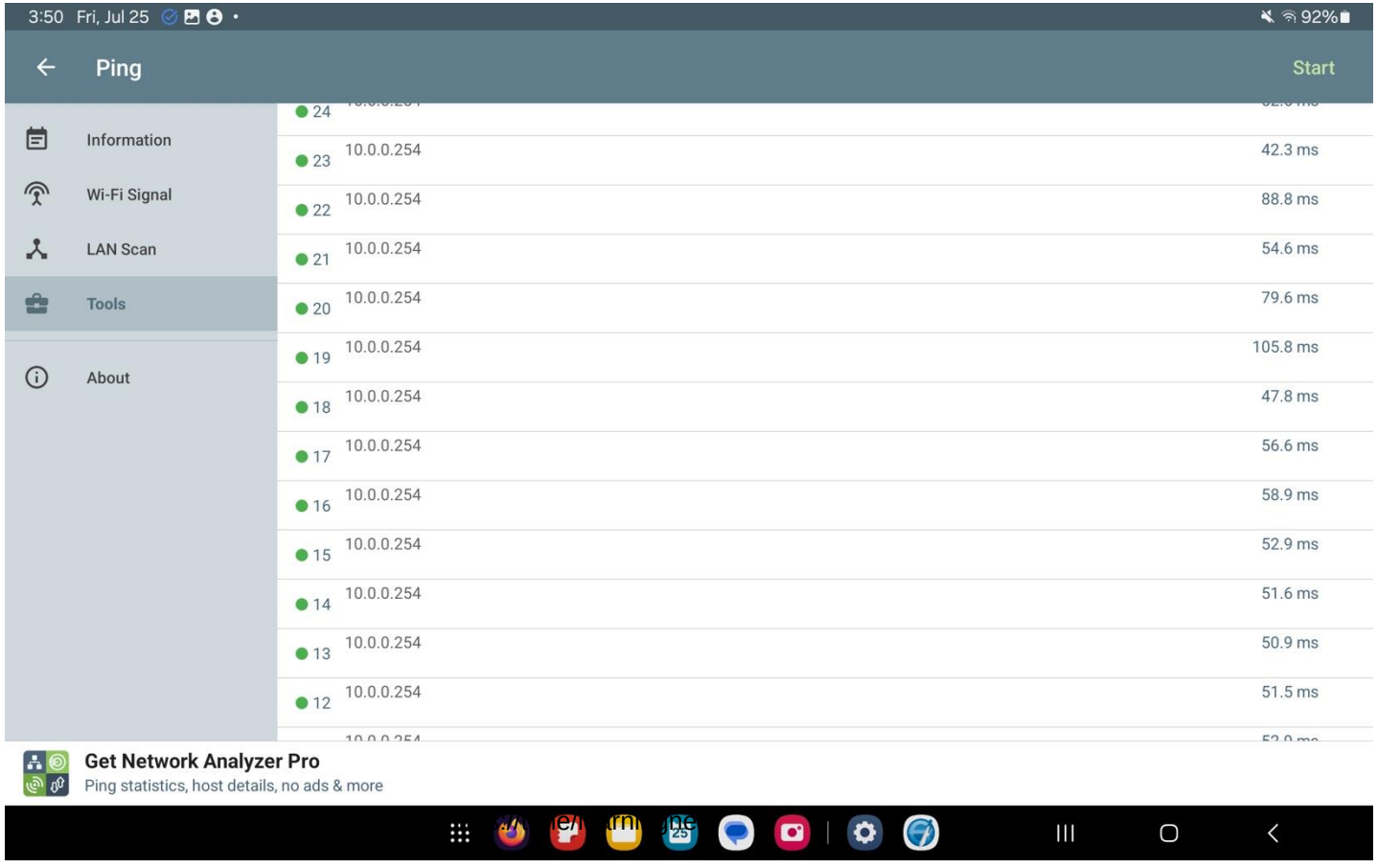
Connected to AP-2

802.1x Re-Authentication

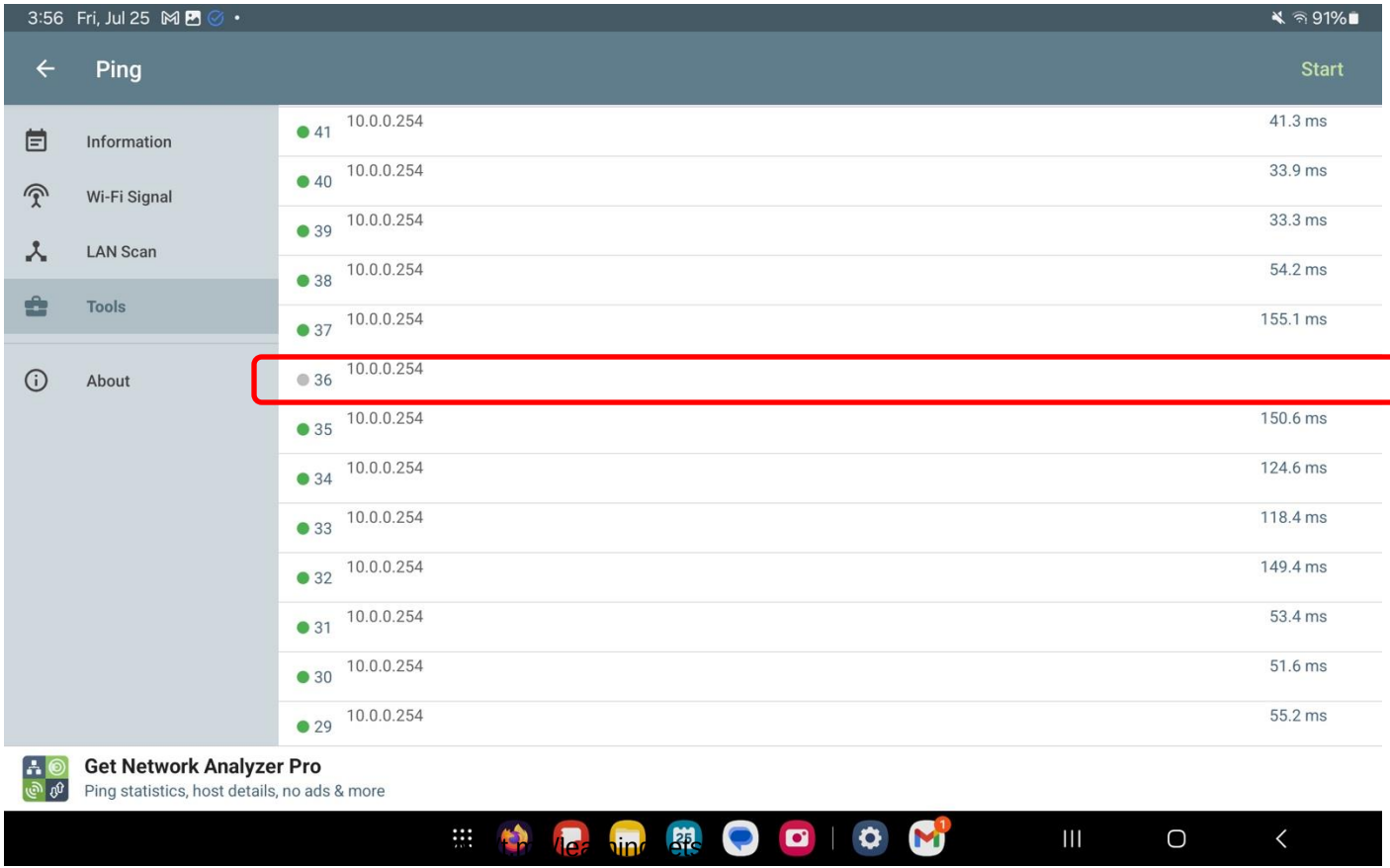
Equidistant between AP-1 and AP-2

Connected to AP-1 (avg = 53.56 ms)

WPA PSK Roaming WITH Mobility Tunnel



802.1x Roaming WITH Mobility Tunnel



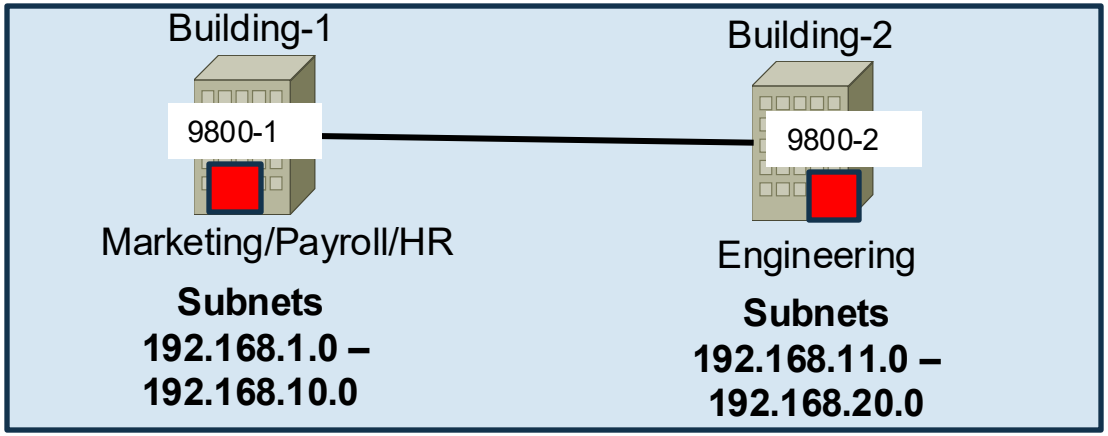
Benefits of Mobility Groups

- 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!!

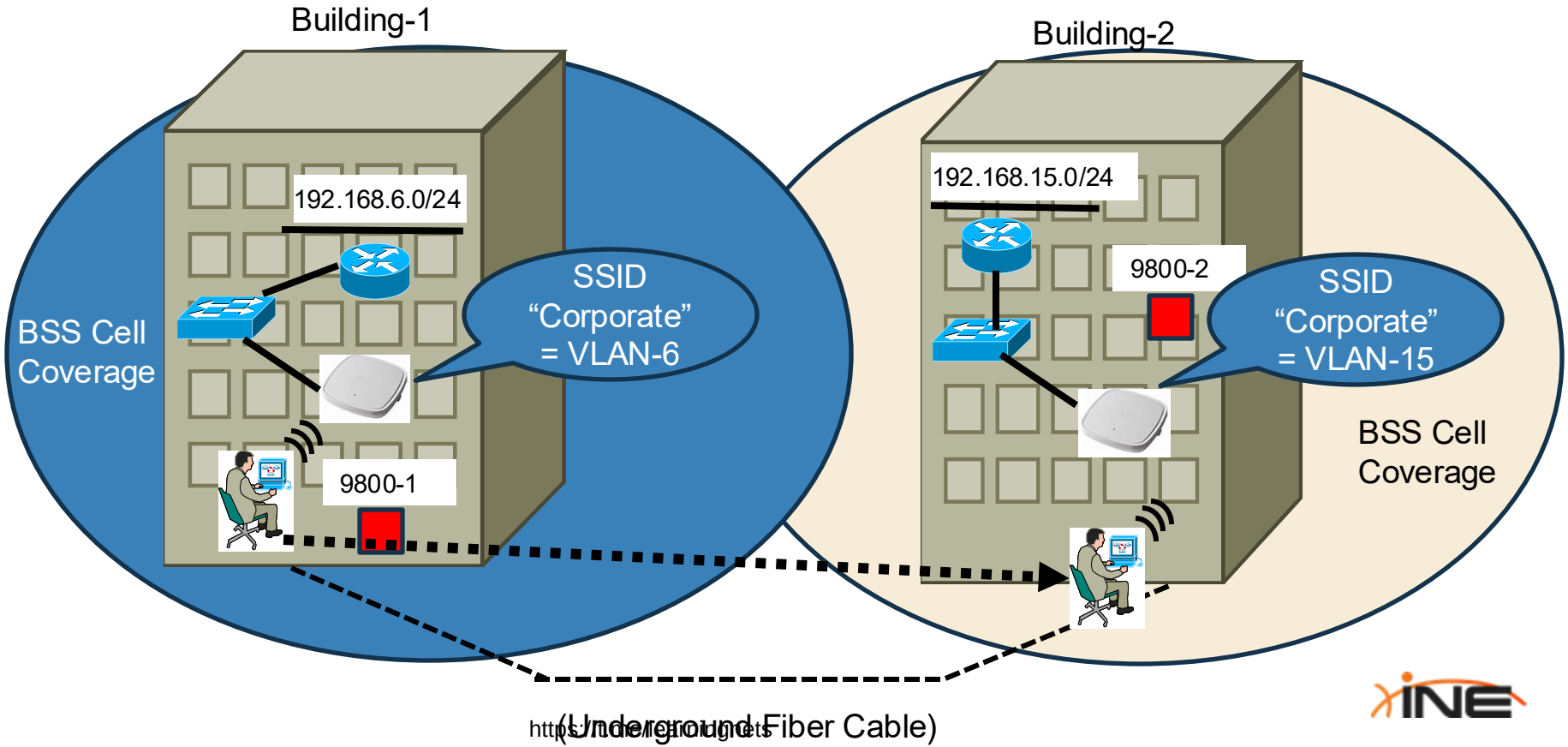
Layer-3 Inter-Controller Roaming

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



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

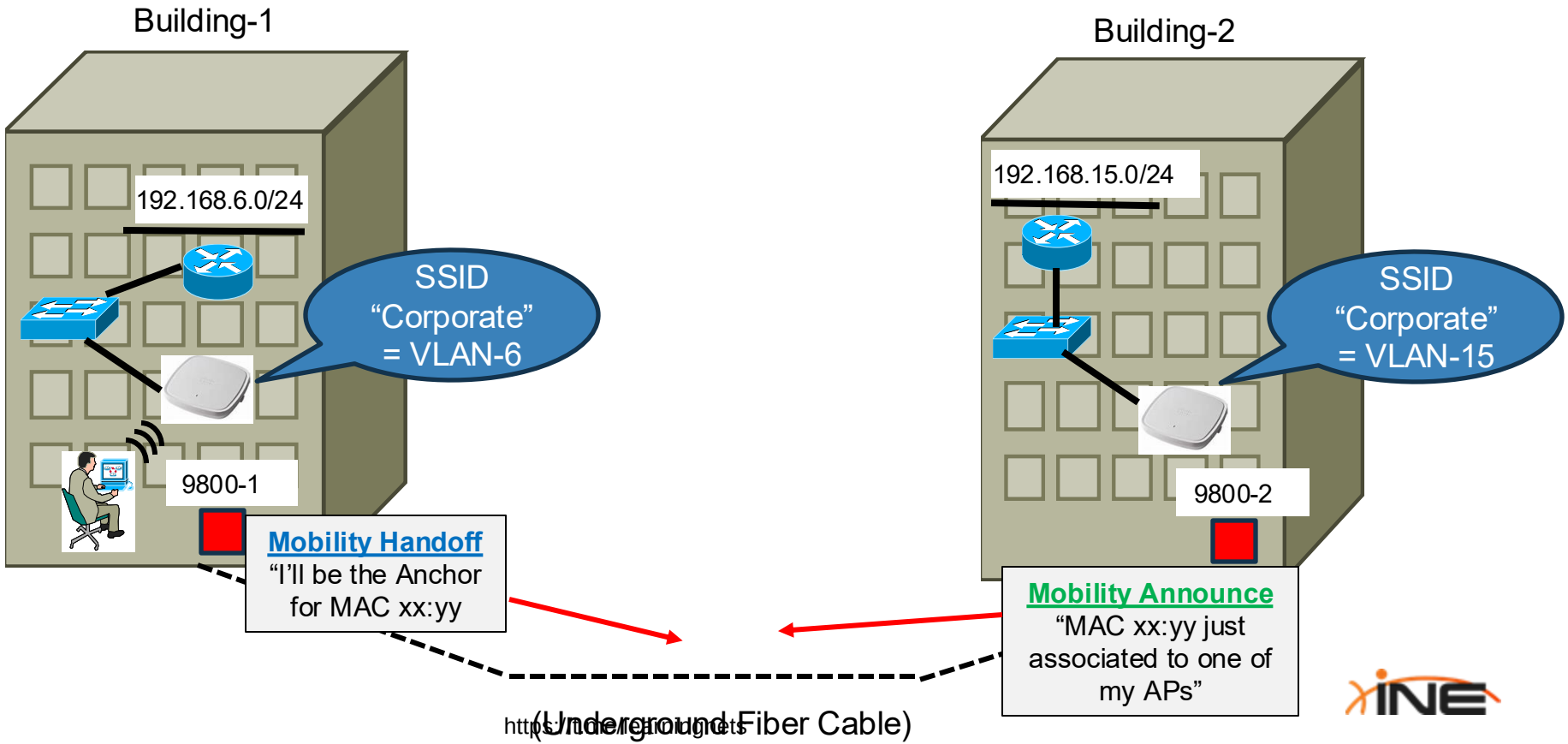
Anchor & Foreign

- 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

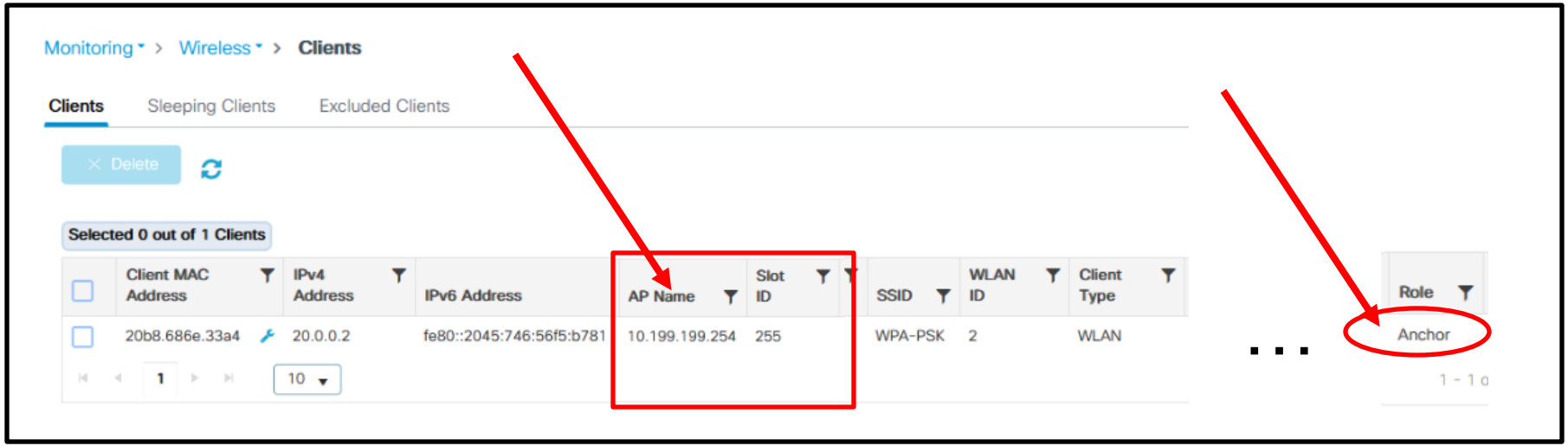
- Anchor continues switching traffic into the distribution system (wired network)
- The client entry exists on both controllers:
  - Marked as “Anchor” on the original controller (where the client first connected)
  - Marked as “Foreign” on the controller the client roamed to
- Client maintains its original 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

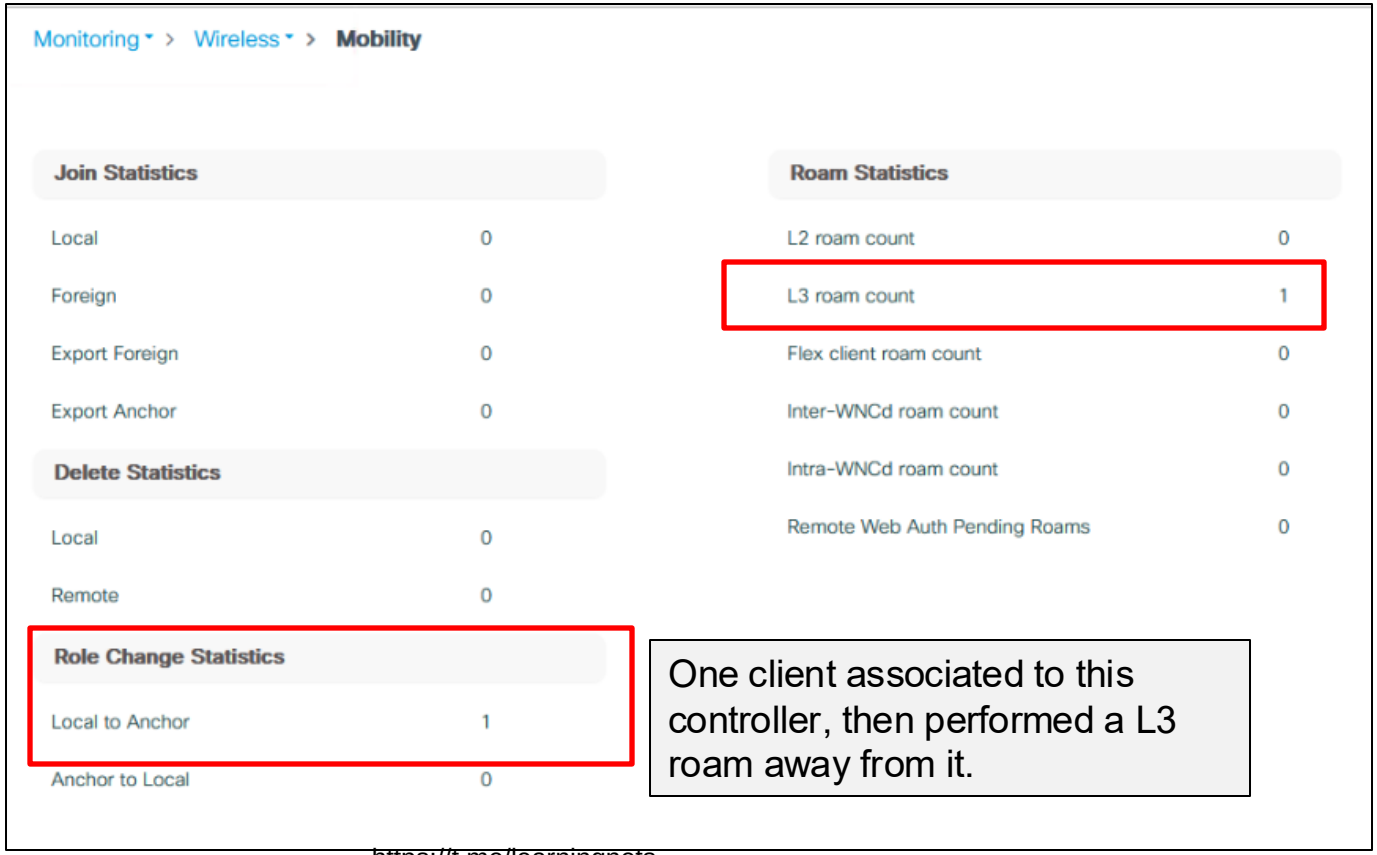
- Upon first association to an access point…



- 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

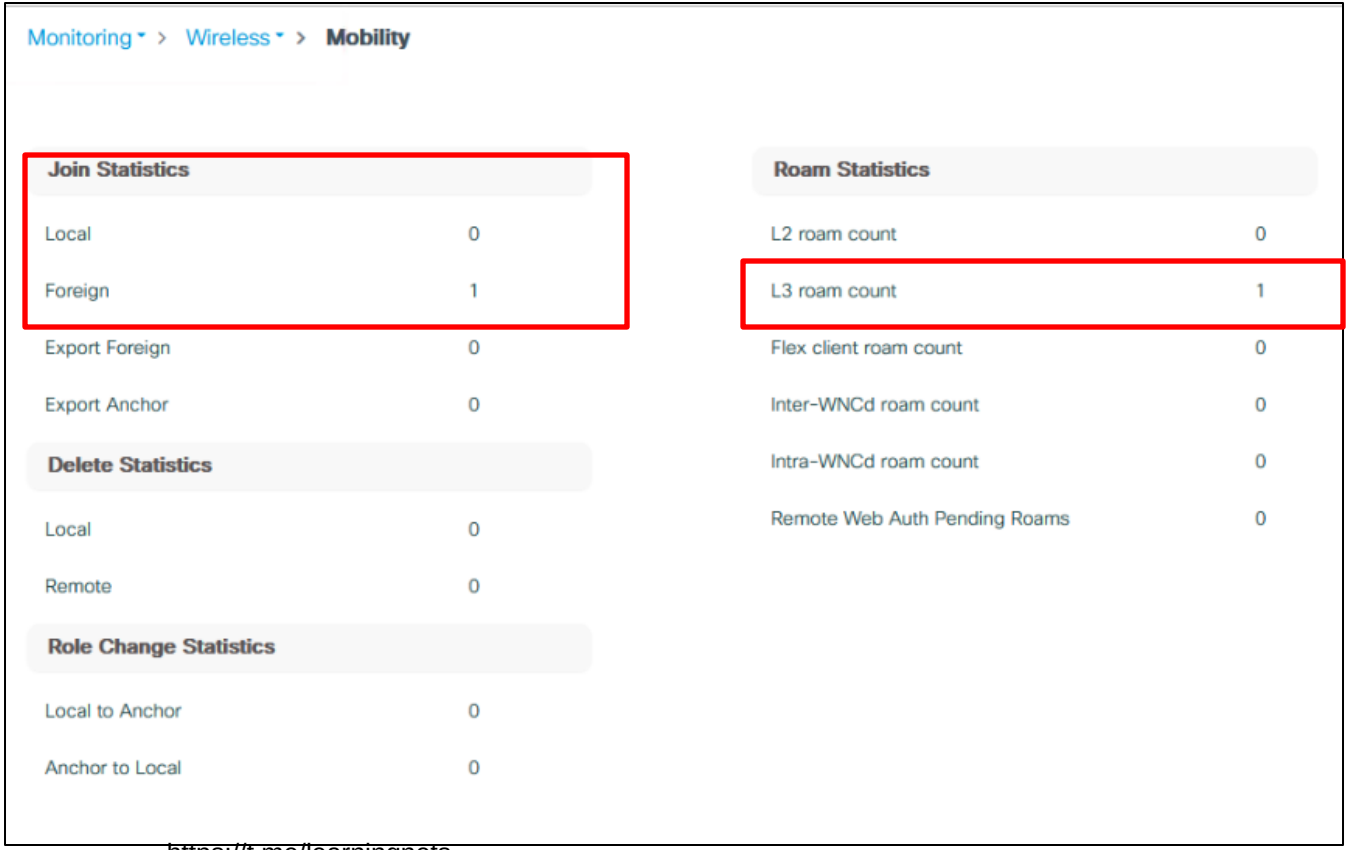
Monitoring Mobility (9800)



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.



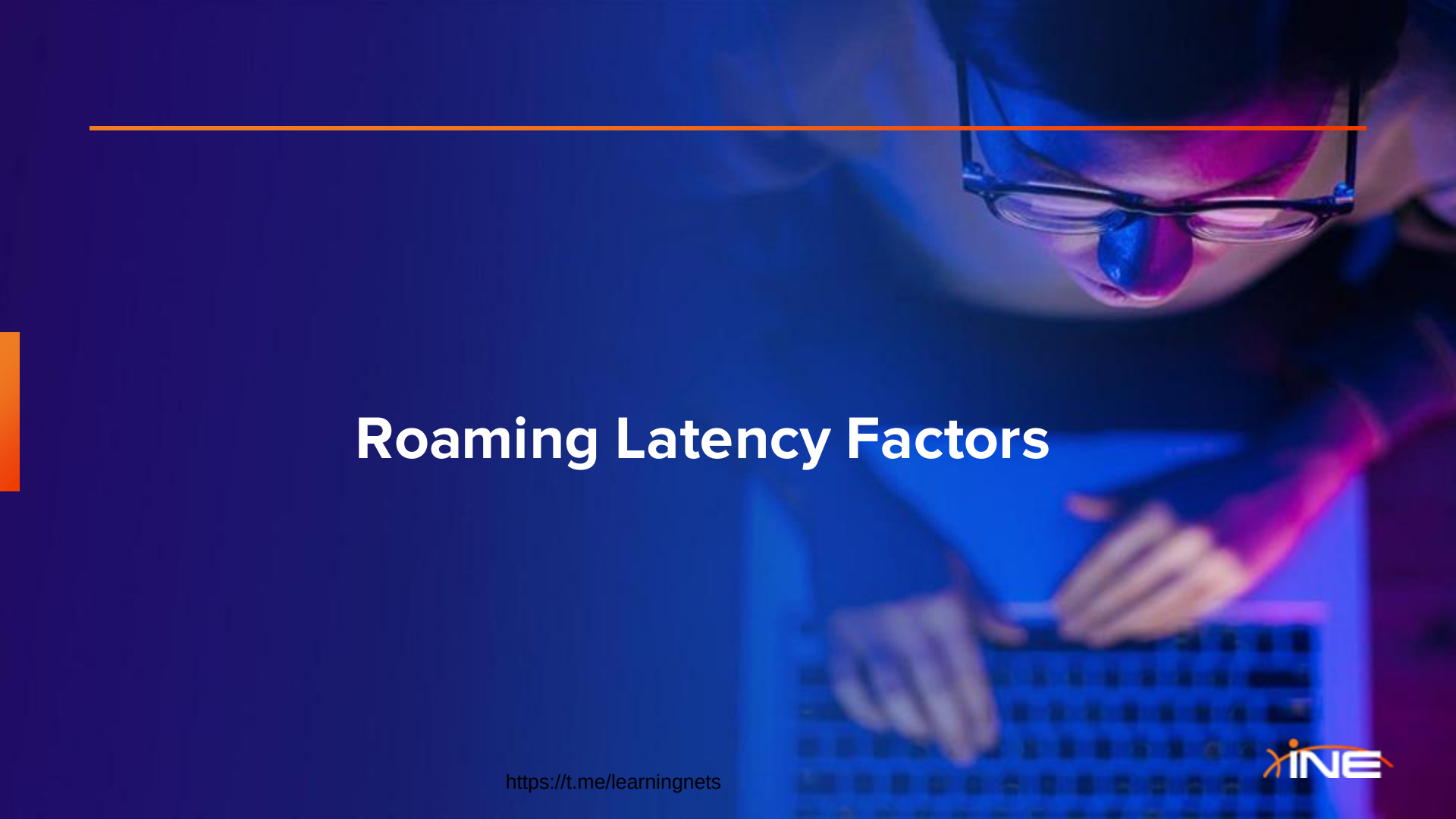
Monitoring Client Mobility History

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

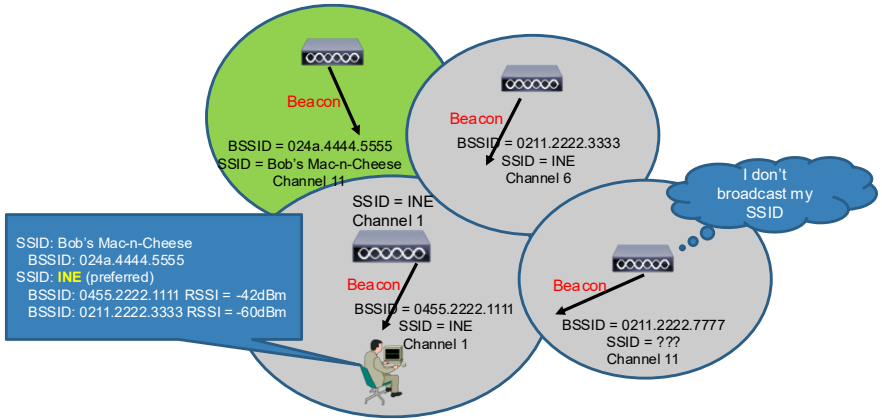
General Factors That Affect Roaming

- 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

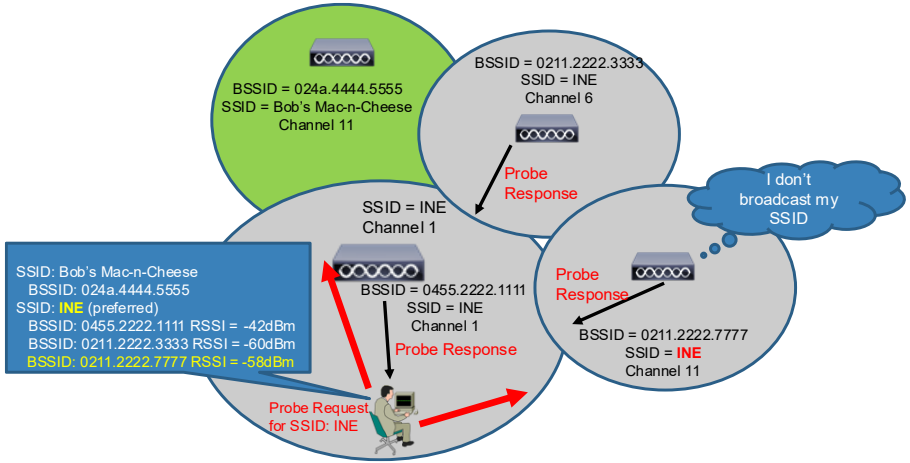
- Delay-sensitive apps (e.g., voice, timeout-sensitive apps) may experience issues during roaming
- User may perceive:
  - Audio gaps
  - Application disconnects
  - Pauses in video
- Severity depends on how quickly the client resumes sending/receiving data

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)

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

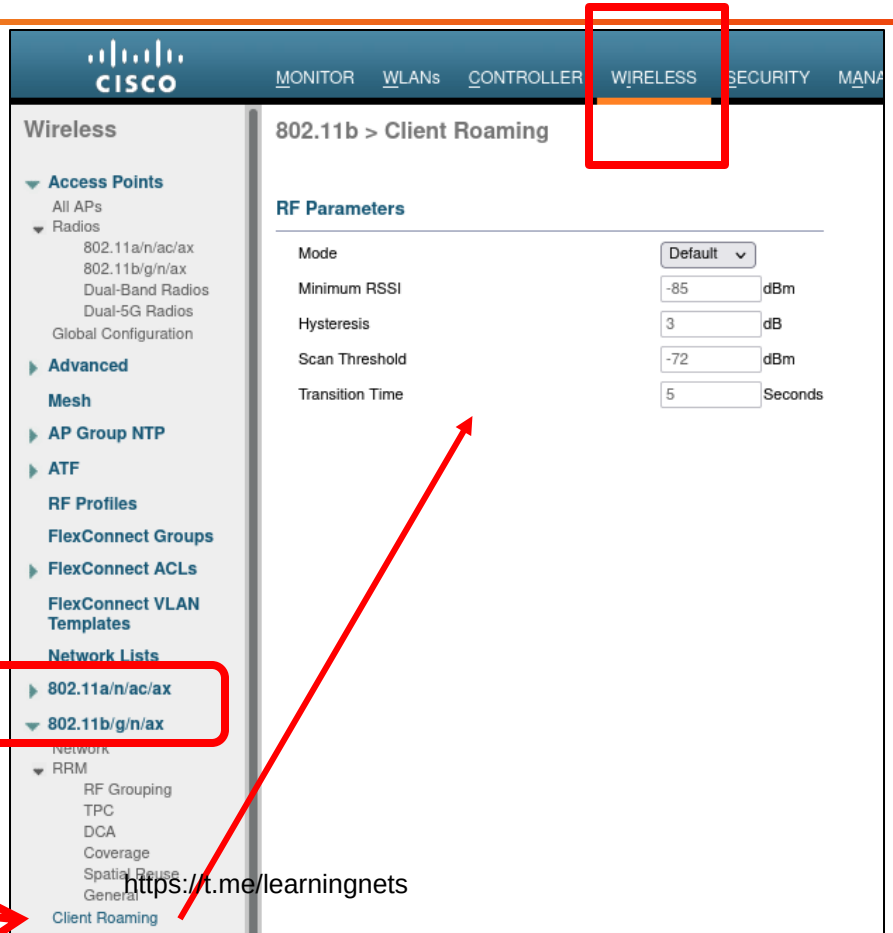
What Problem Does CCX Solve?

- 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



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

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

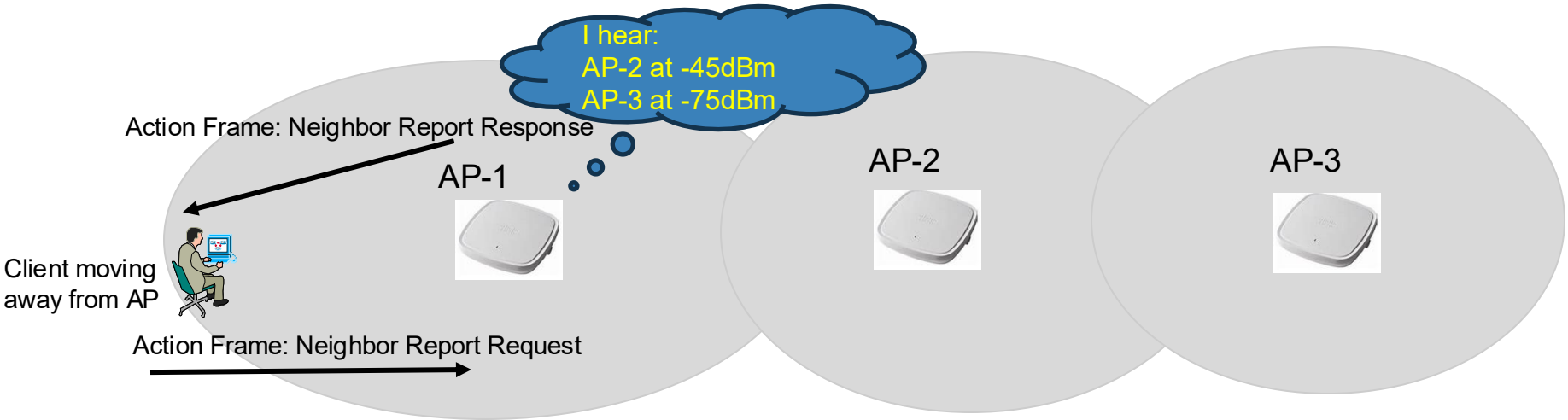
- IEEE first begins working on 802.11k in 2006
- Finalized and ratified as an official standard in 2008
- Gained traction after adoption by Wi-Fi Alliance's Voice-Enterprise certification
- Included in modern Wi-Fi chipsets and supported in Wi-Fi 4, 5, 6, and 6E clients

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
⌄ 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]
⌄ IEEE 802.11 Wireless Management
  ⌄ Fixed parameters
      Category code: Radio Measurement (5)
      Action code: Neighbor Report Request (4)
      Dialog token: 1
  ⌄ Tagged parameters (9 bytes)
    ⌄ Tag: SSID parameter set: "WPA-PSK"
        Tag Number: SSID parameter set (0)
        Tag length: 7
        SSID: "WPA-PSK"
```

Neighbor Report Response

```
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)
  .... .... .... 0000 = Fragment number: 0
  0010 1111 1101 .... = Sequence number: 765
  Frame check sequence: 0x34931a77 [unverified]
  [FCS Status: Unverified]
  [WLAN Flags: ........C]
IEEE 802.11 Wireless Management
  Fixed parameters
    Category code: Radio Measurement (5)
    Action code: Neighbor Report Response (5)
    Dialog token: 1
  Tagged parameters (15 bytes)
    Tag: Neighbor Report
      Tag Number: Neighbor Report (52)
      Tag length: 13
      BSSID: Cisco_89:09:ef (7c:21:0d:89:09:ef)
      BSSID Information: 0x000002f7
      Operating Class: 118
      Channel Number: 64 (iterative measurements on that Channel Number)
      PHY Type: 0x07
```

Current AP's BSSID

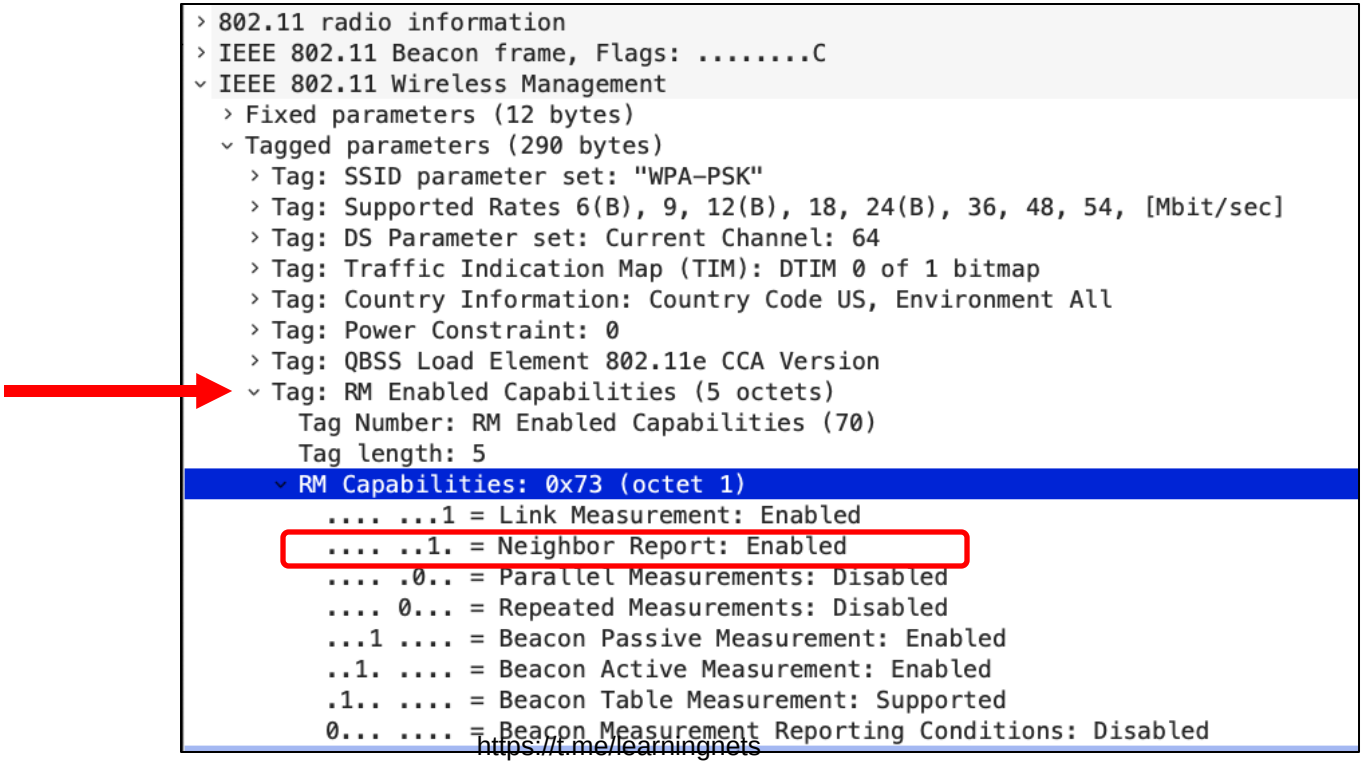
Neighbor AP's BSSID

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-assocation Request frames

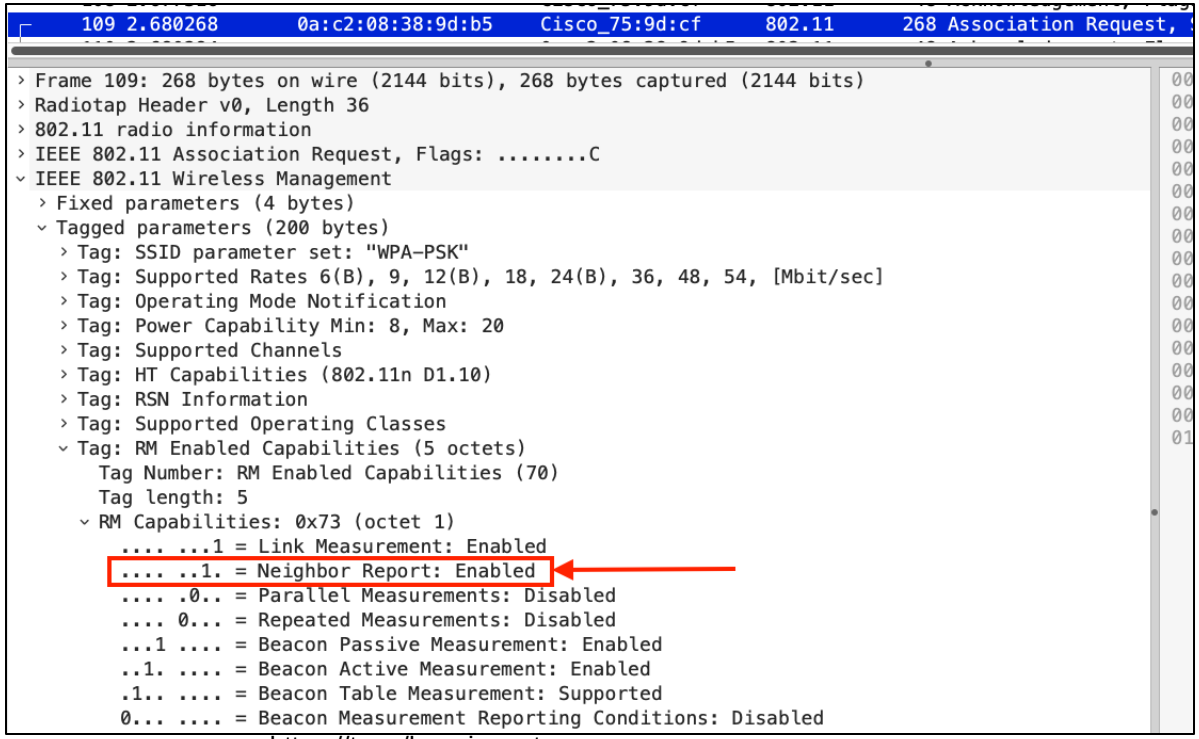
Verifying 802.11k Access Point Support

- 802.11k “Neighbor List” support advertised in Beacons



Verifying 802.11k WLAN Client Support

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

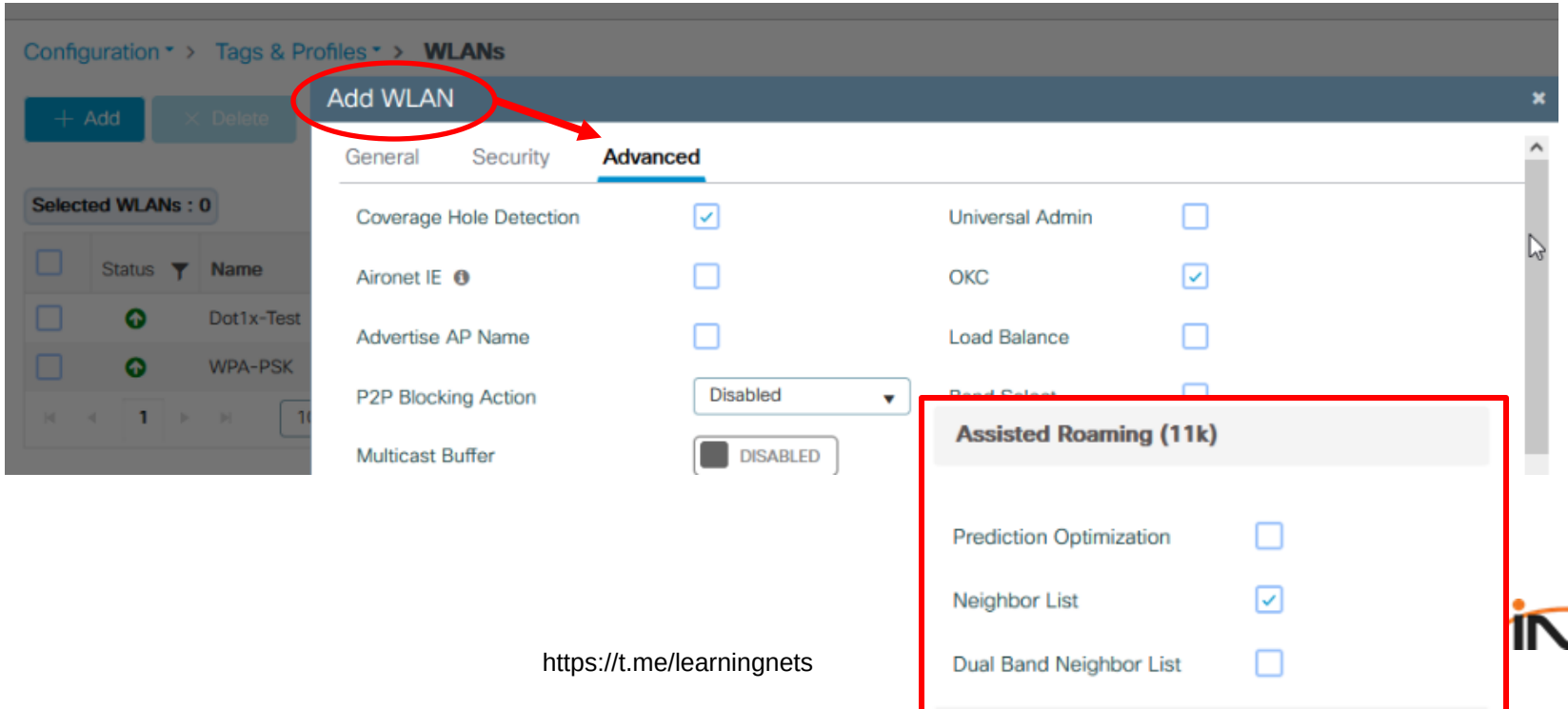


Cisco Catalyst 9800 Support

- 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



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

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

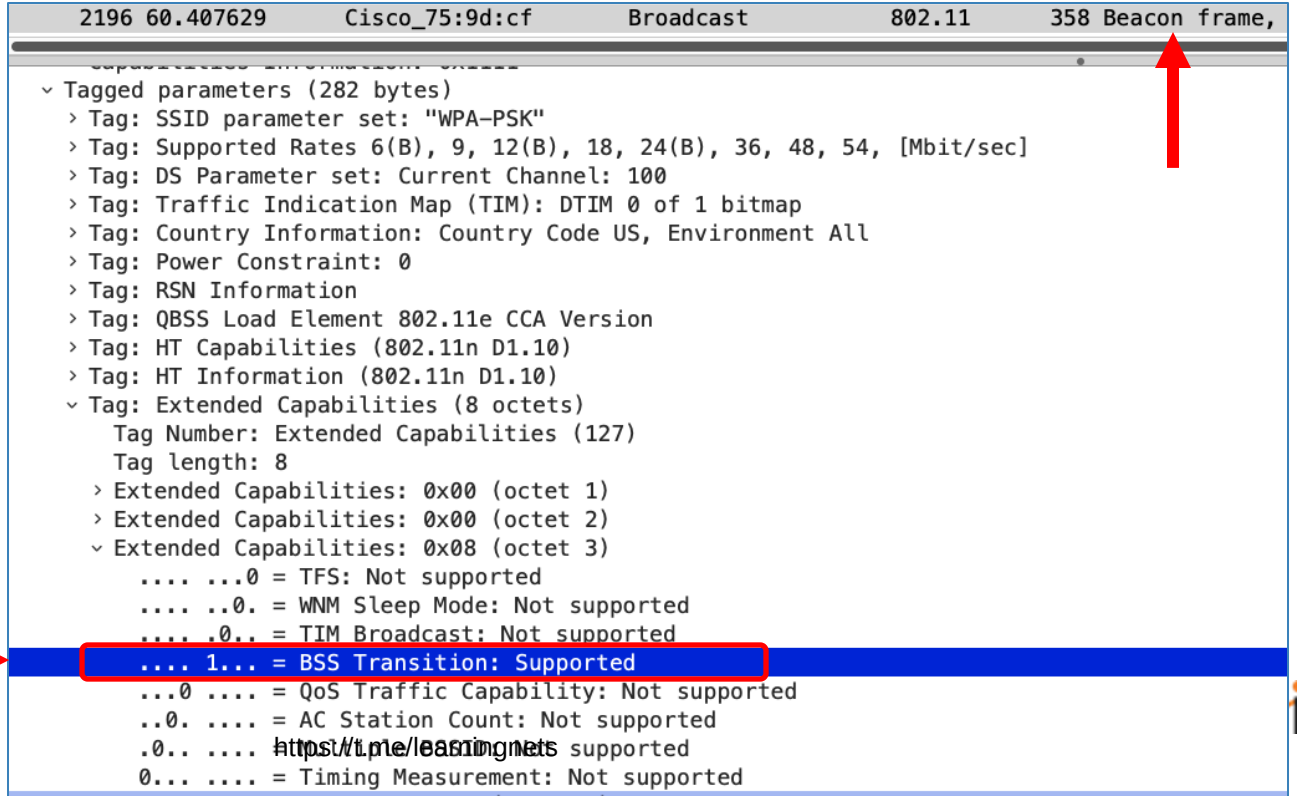
- AP-initiated or client-initiated roaming suggestions:
  - AP sends a *BSS Transition Management Request*
  - Client may send a *BSS Transition Management Query* (solicited request)
- Candidate list of AP's with the current AP's "Request" includes:
  - BSSID, Channel, Preference value
- Client responds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

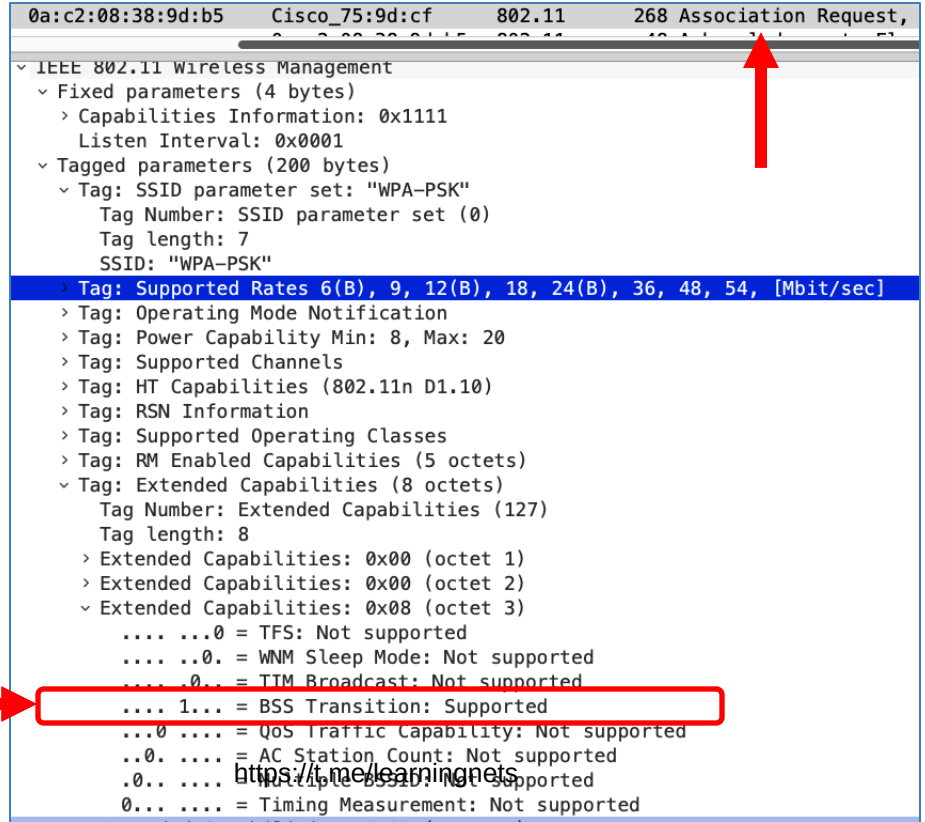
Verifying 802.11v Access Point Support

- 802.11v “BSS Transition” support advertised in Beacons



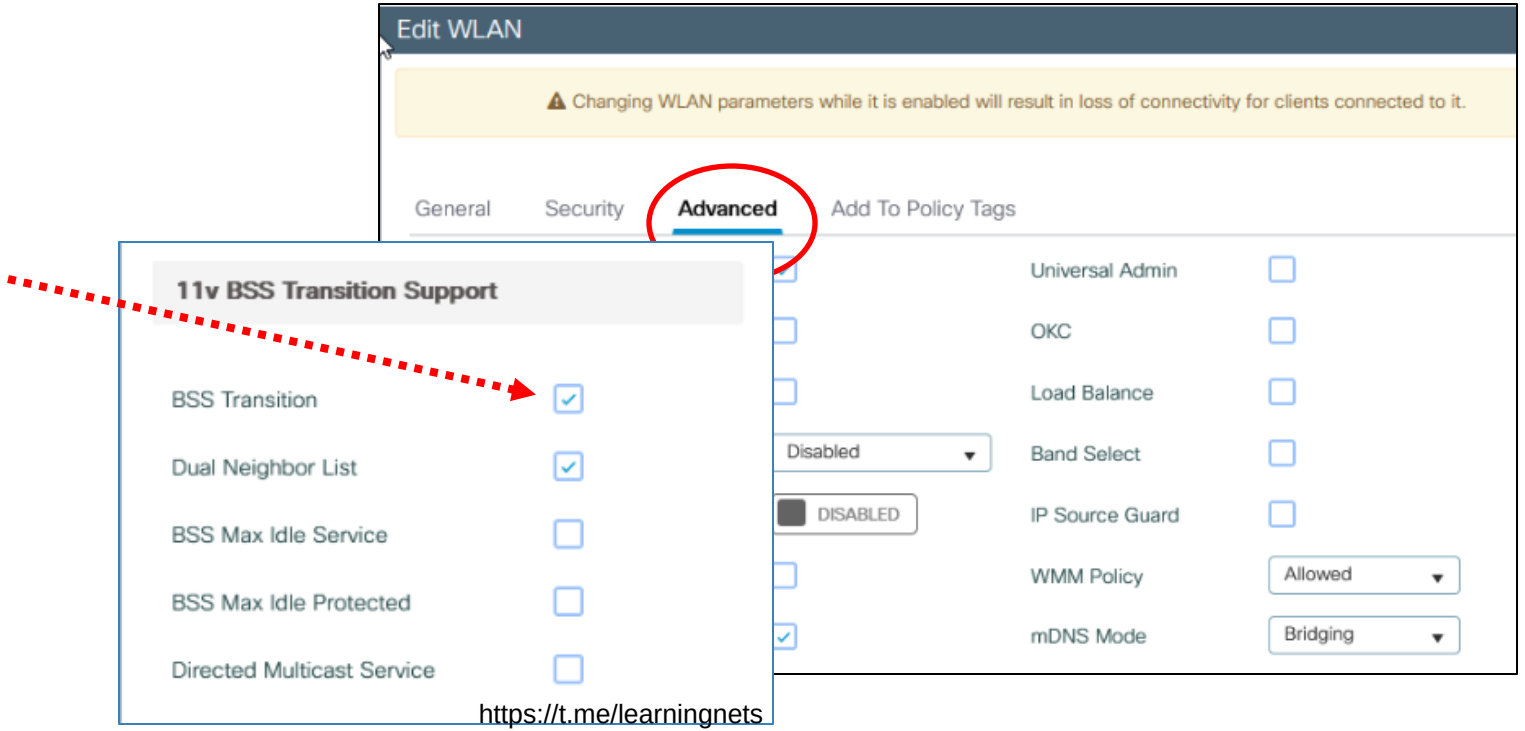
Verifying 802.11v WLAN Client Support

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



Enabling 802.11v on Catalyst 9800s

- 802.11v BSS-Transition enabled by default



Thank you for watching!!

The Robust Security Network

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

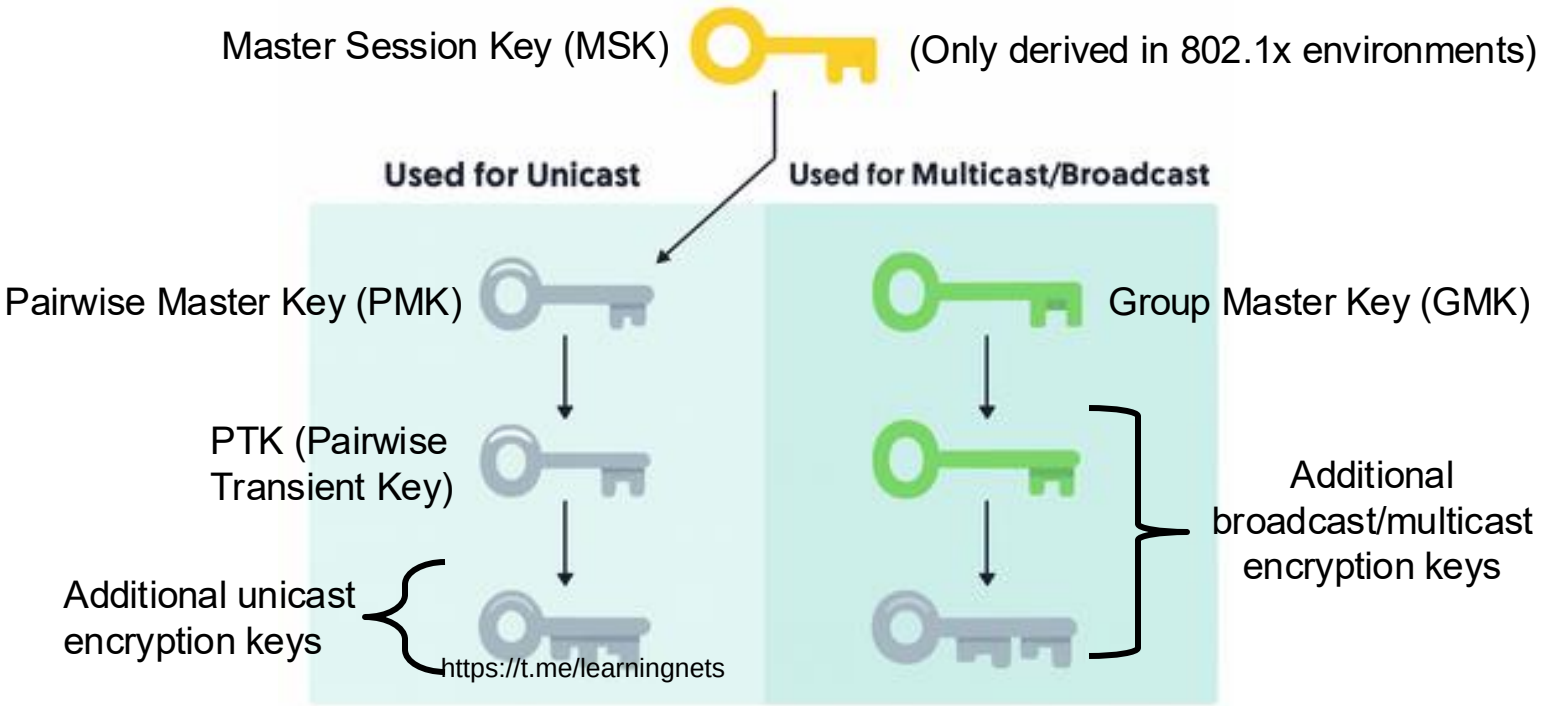
- RSN was introduced in 802.11i
  - *RSN = Wireless networks that leverage cryptography to provide data integrity and confidentiality between WLAN client and AP*
  - Utilizes a hierarchy of cryptographic keys generated, and used during a wireless session
- Certified by WPA2 or WPA3 to manage key generation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

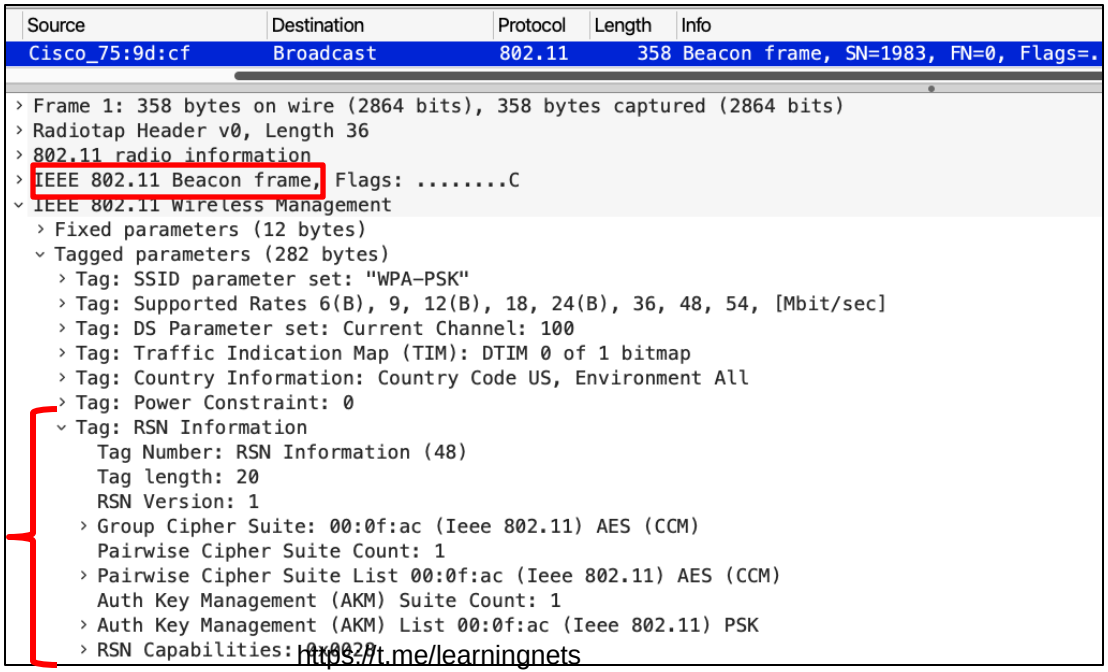
Overview of RSN Keys

- 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.

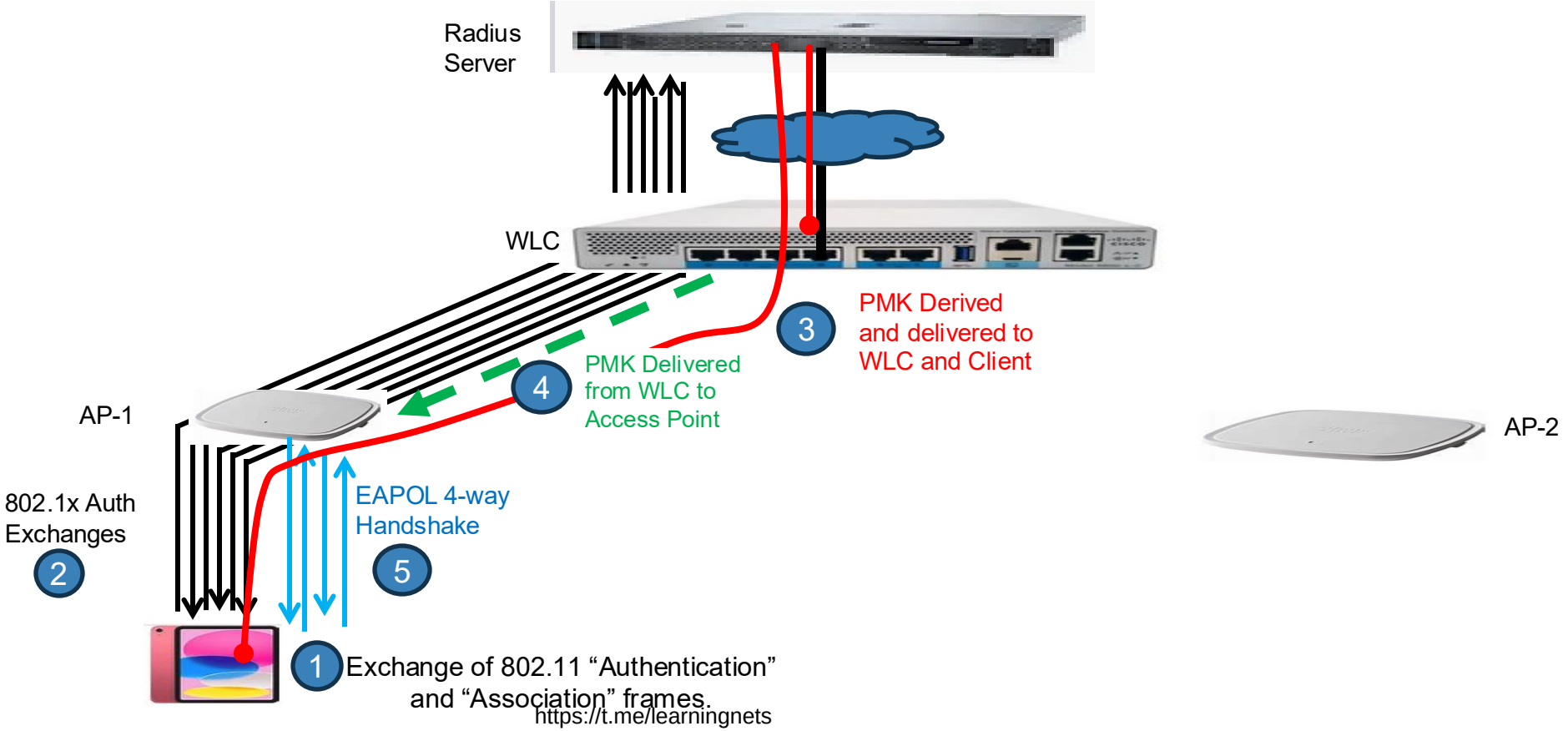


WPA2 / WPA3 Enterprise Association

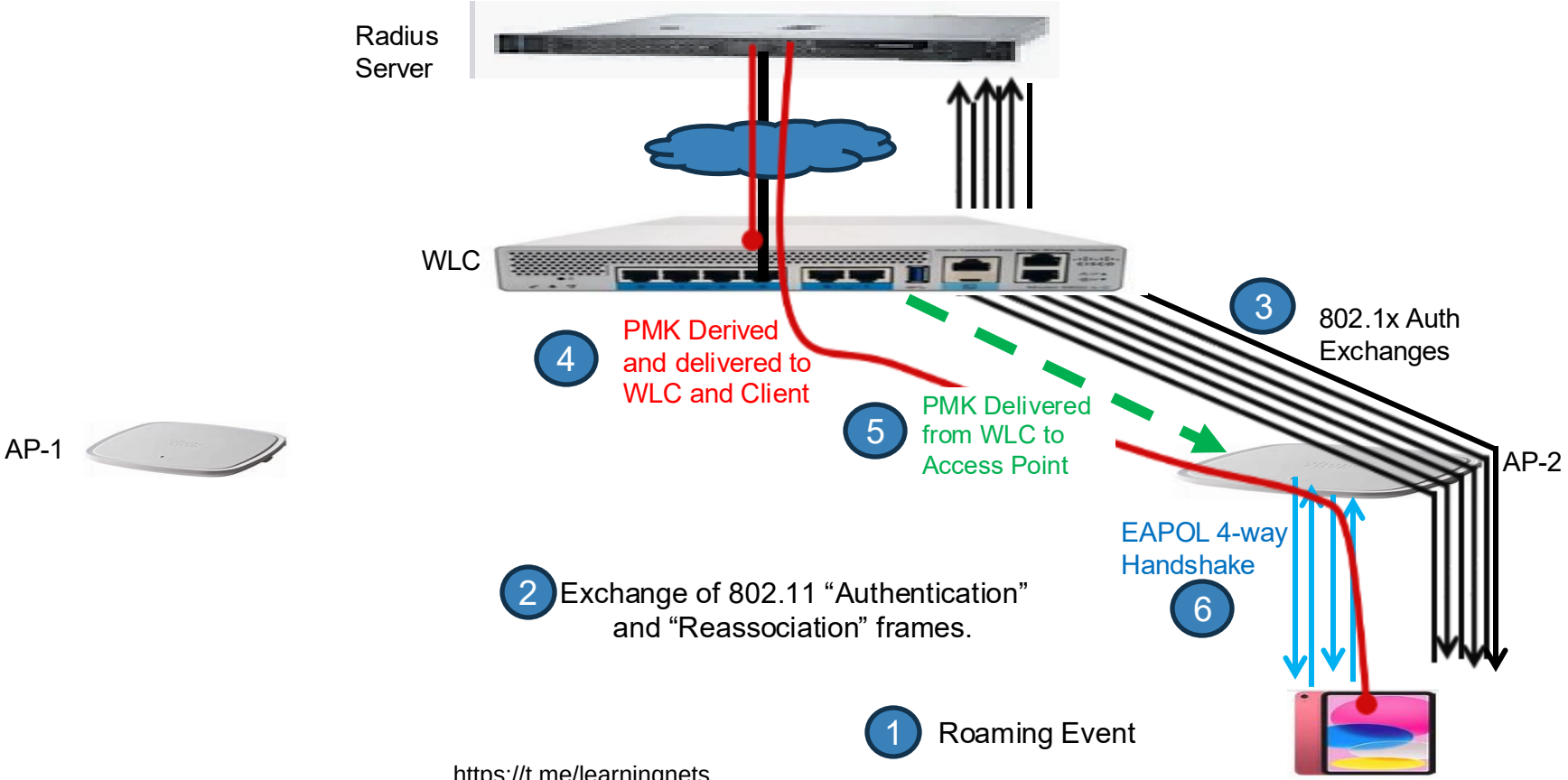
1. 802.11 Authentication and Association messages are exchanged between the AP (or WLC) and the client
2. 802.1x EAP authentication occurs
   a. Client provides security credentials
   b. AP then authenticates against a RADIUS server
   c. This exchange is typically 8-14 messages long
   d. Both the 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



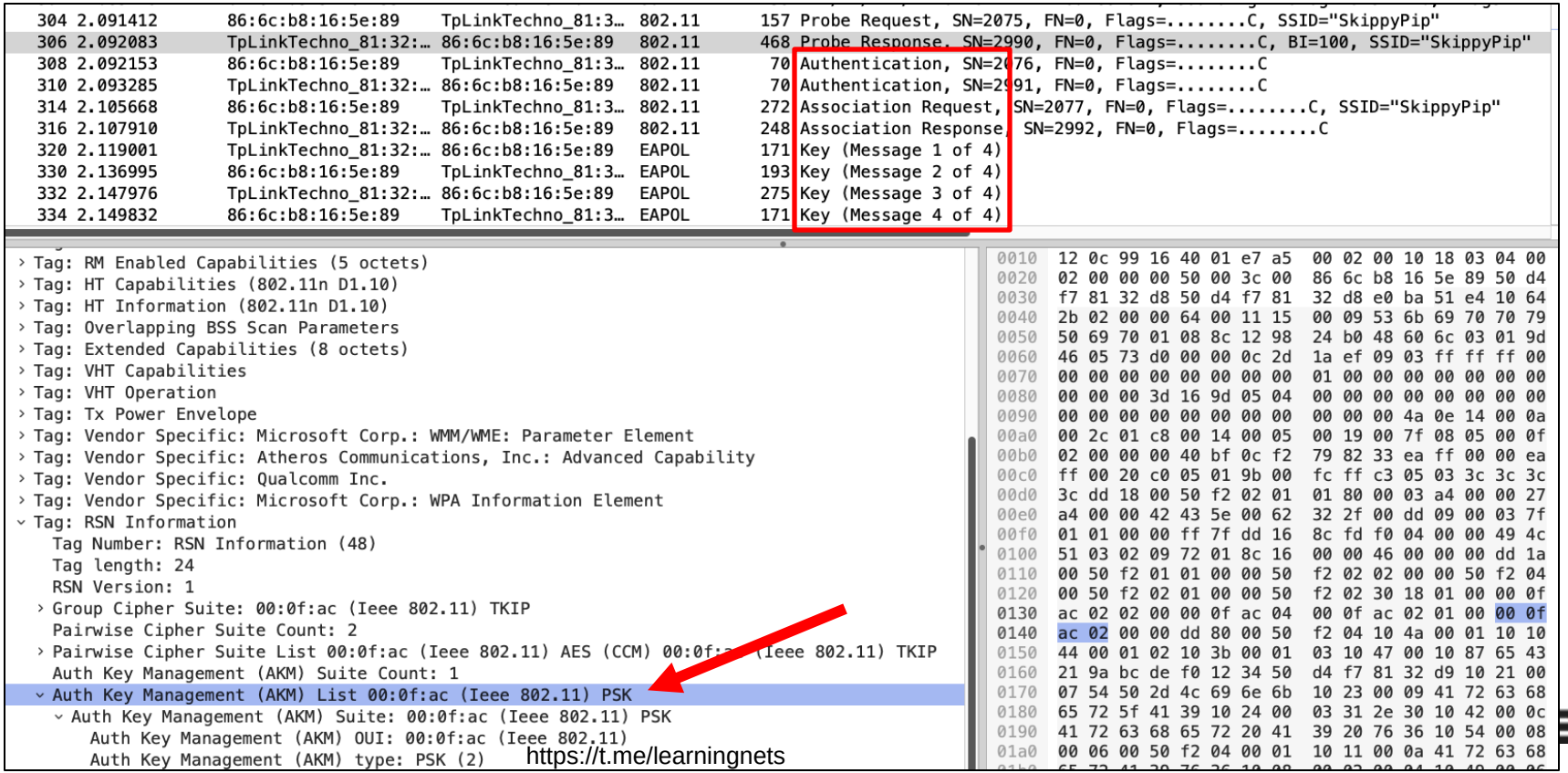
WPA-Enterprise RSN Reassocation Process



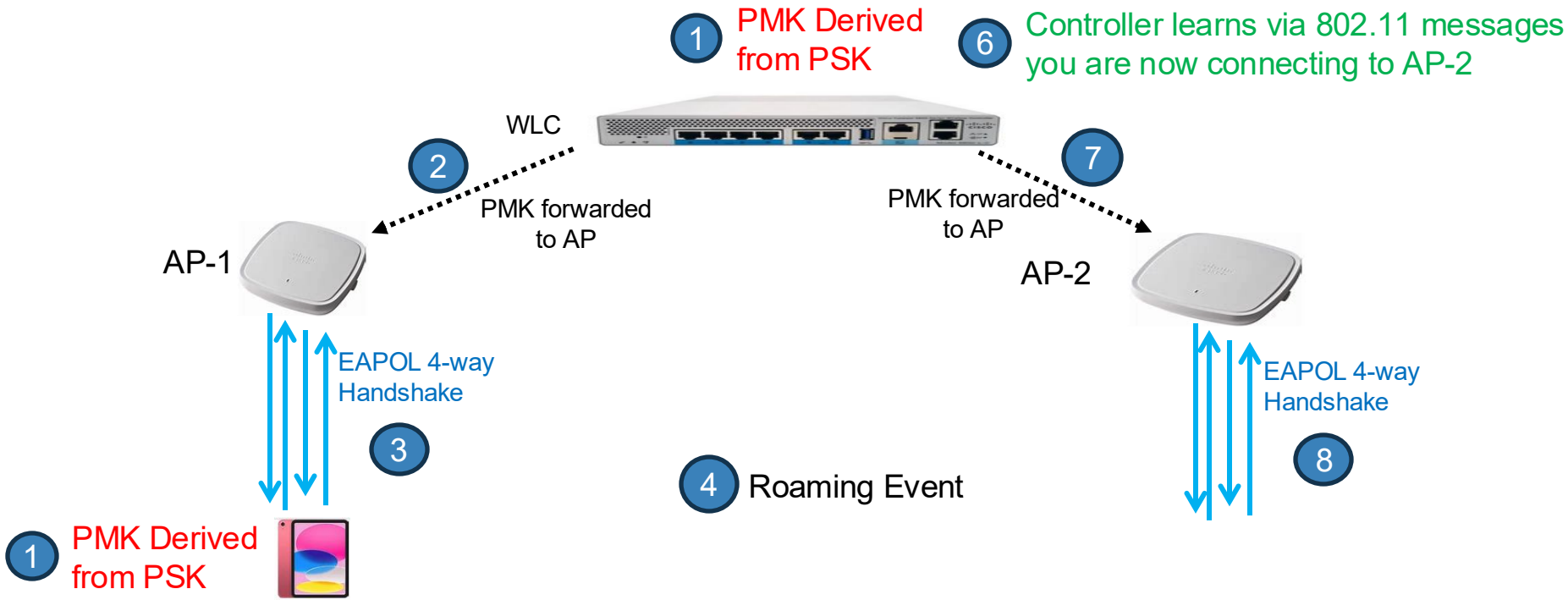
What About WPA-2/WPA-3 Personal?

- 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

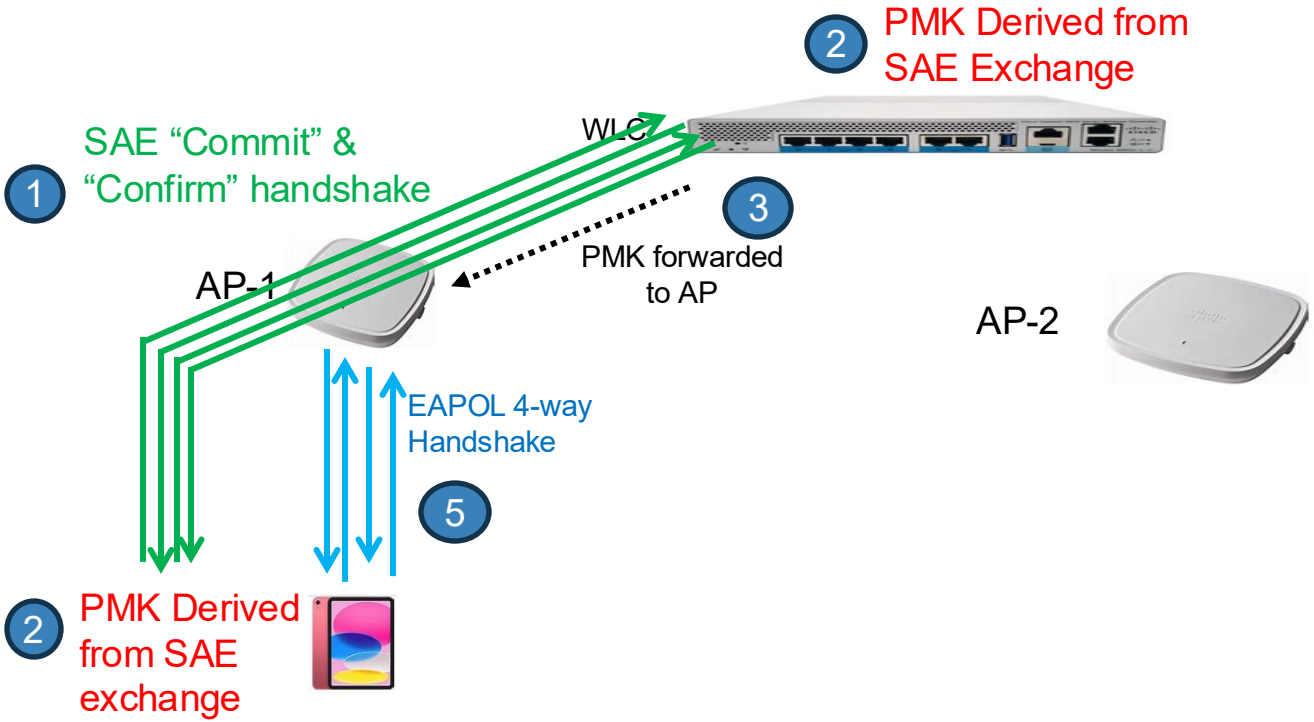
WPA PSK Handshake



WPA-2 Personal Roaming RSN Process



WPA-3 Personal Roaming RSN Process



1 802.11 Authentication contains SAE exchanges

4 802.11 Association Message exchange.

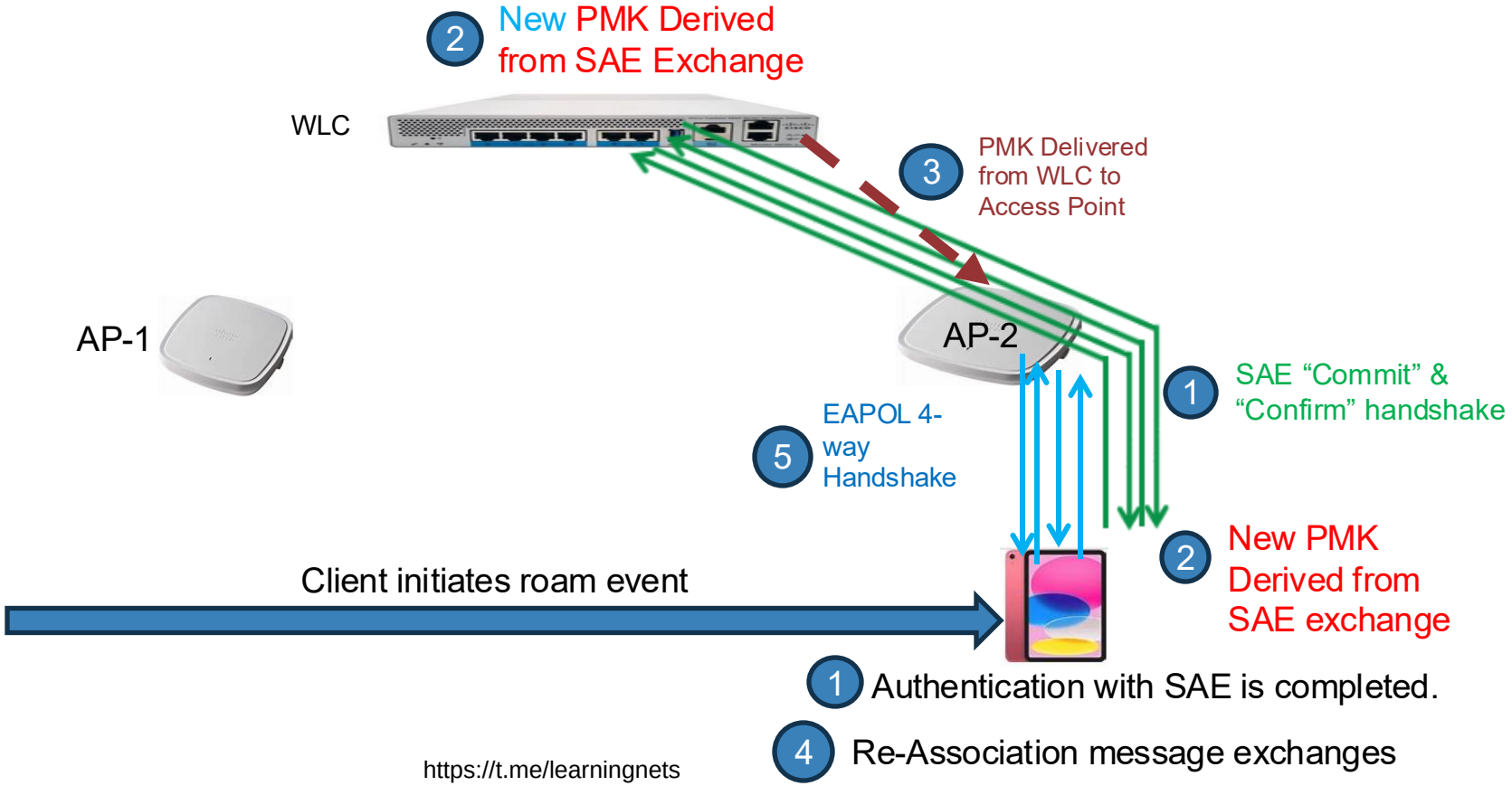
WPA3 SAE Exchanges

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)

```
> 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
v IEEE 802.11 Wireless Management
  v Fixed parameters (104 bytes)
      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
```

```
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
```

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

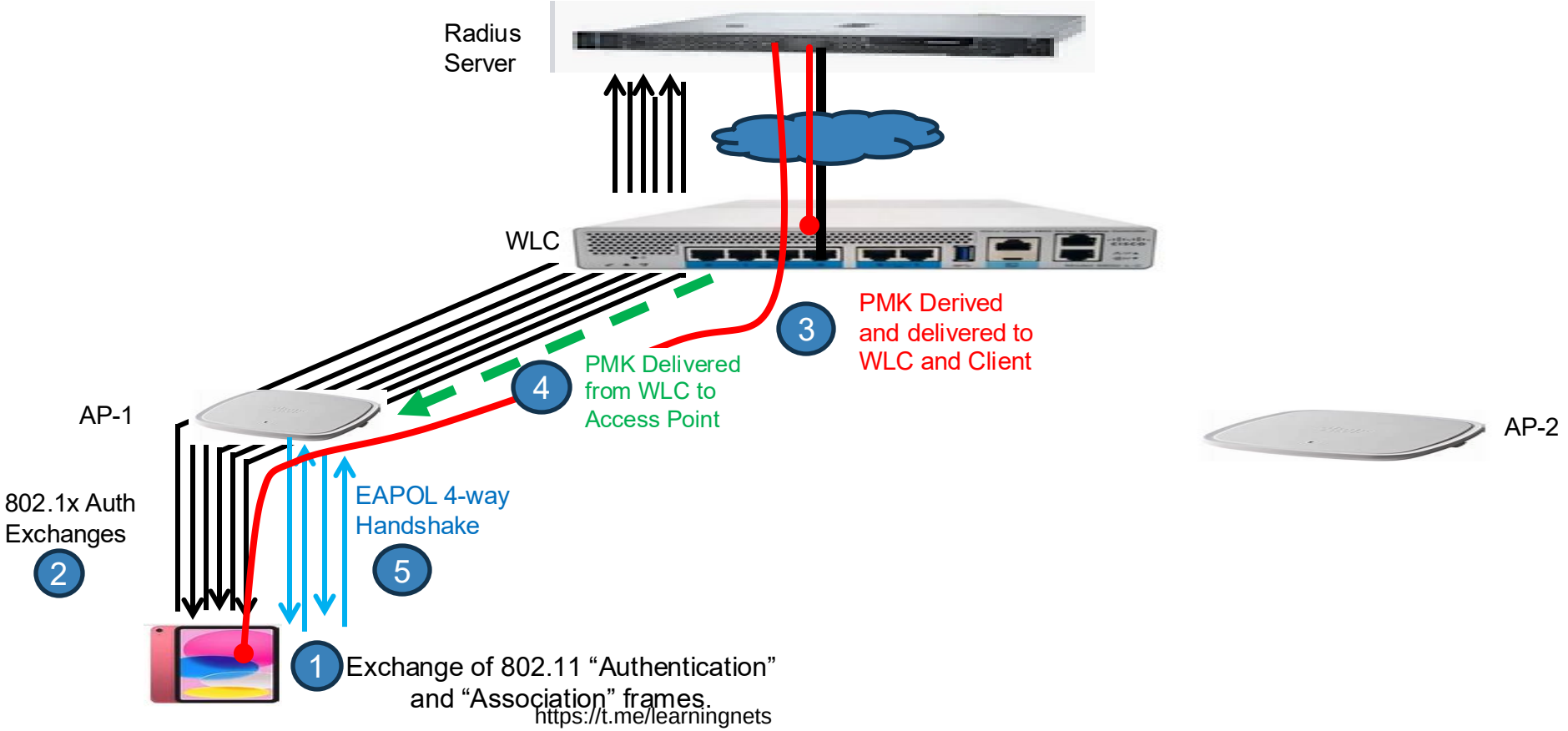
Thank you for watching!!

Cisco Centralized Key Management (CCKM)

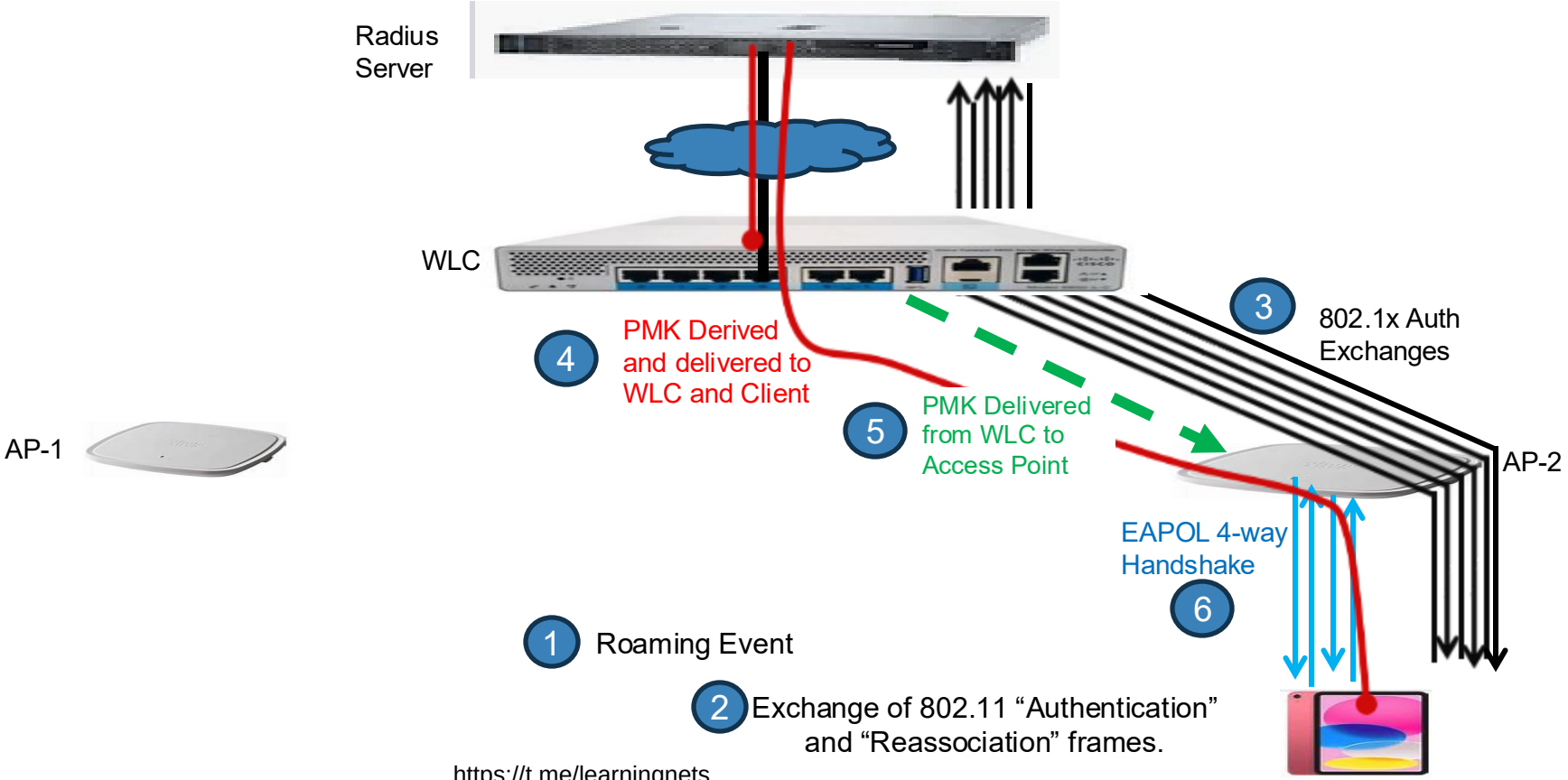
CCKM Overview

- 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



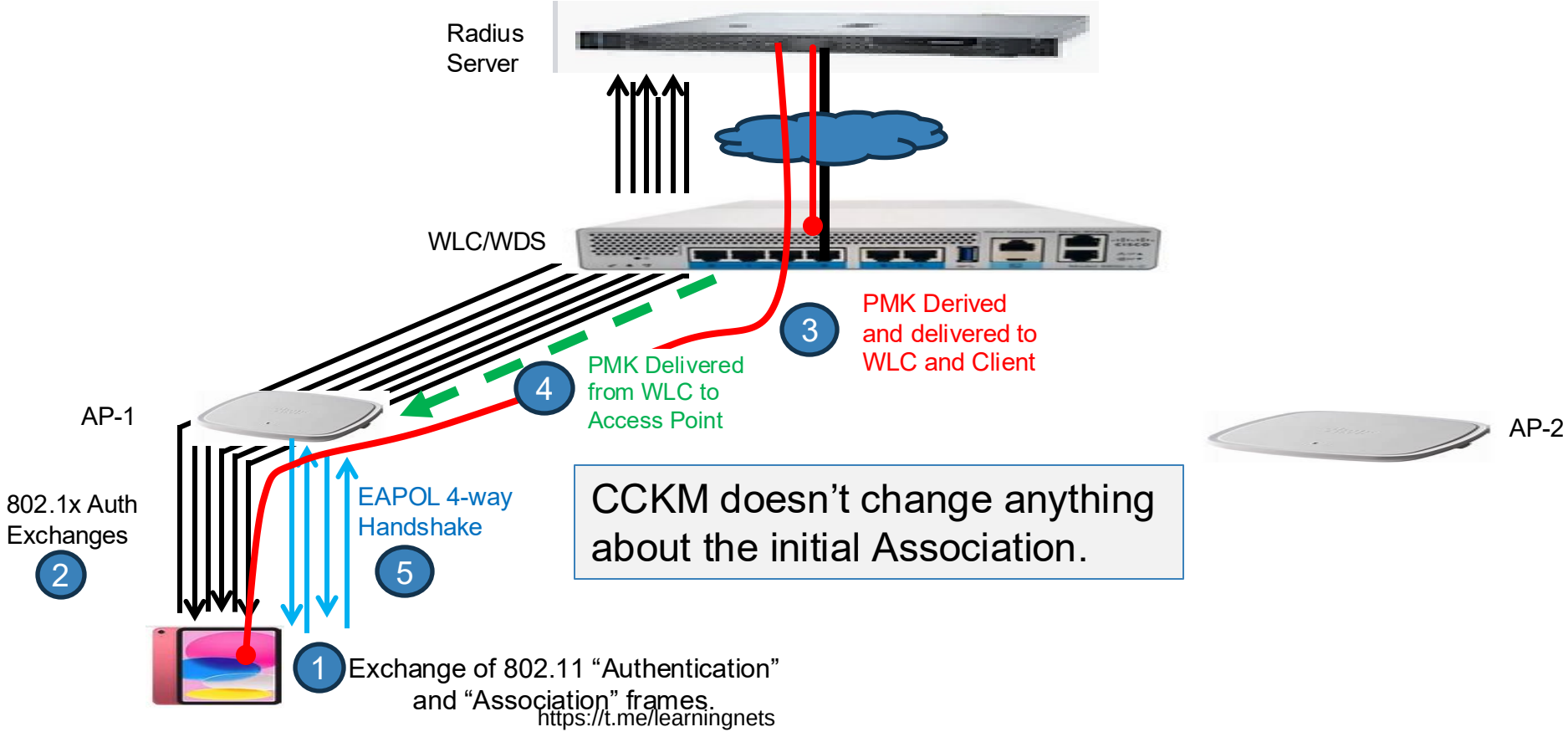
WPA-Enterprise RSN Reassocation Process



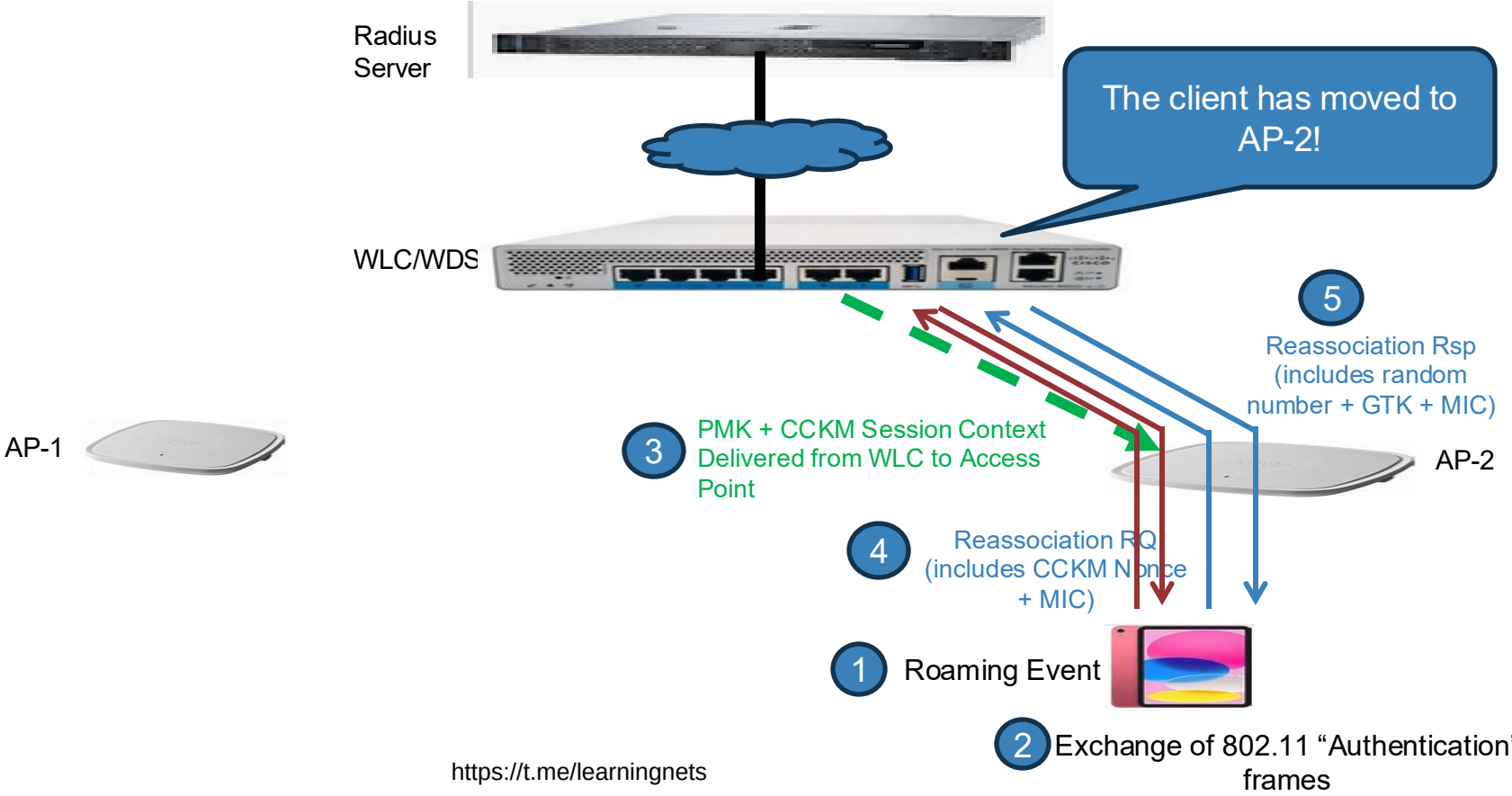
CCKM Operation

- 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

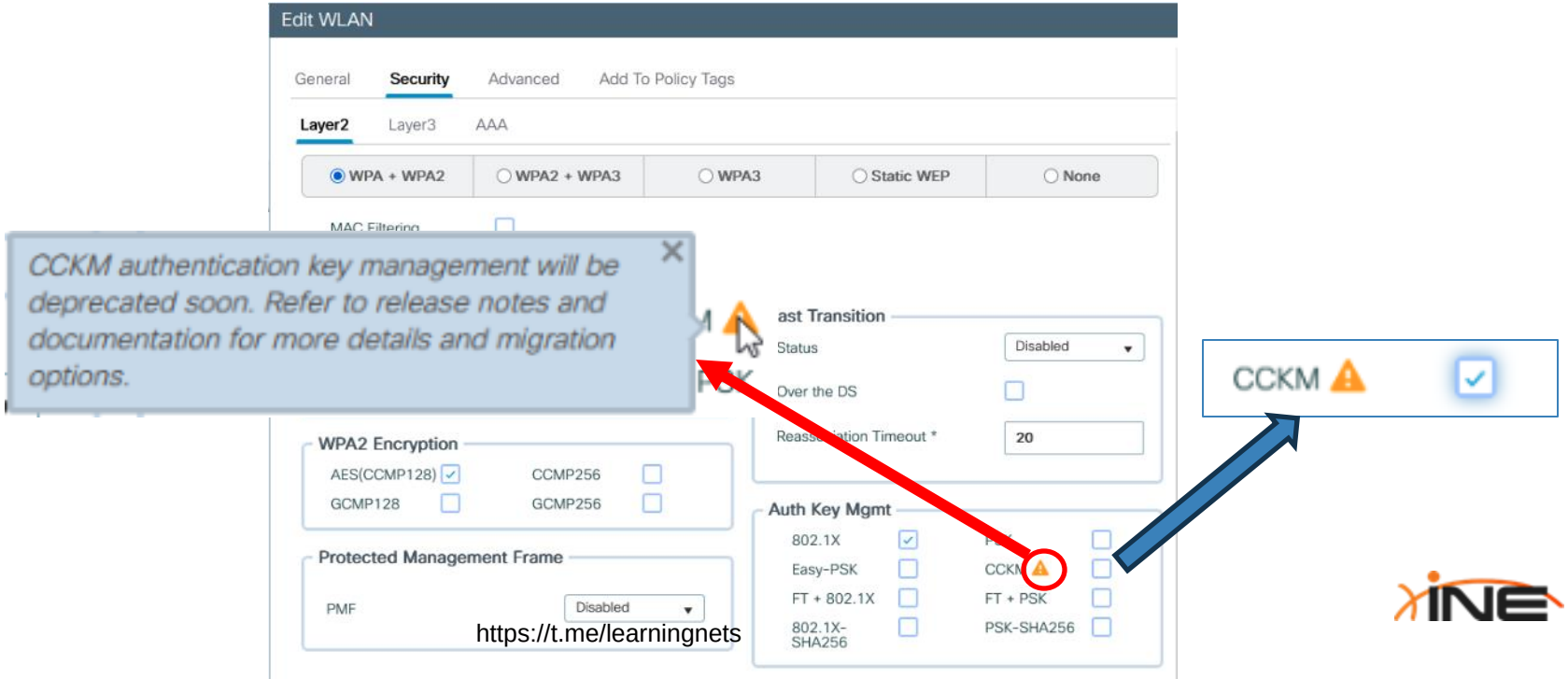


Optimized Roaming with CCKM



Enabling CCKM

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



Thank you for watching!!

Opportunistic Key Caching (OKC)

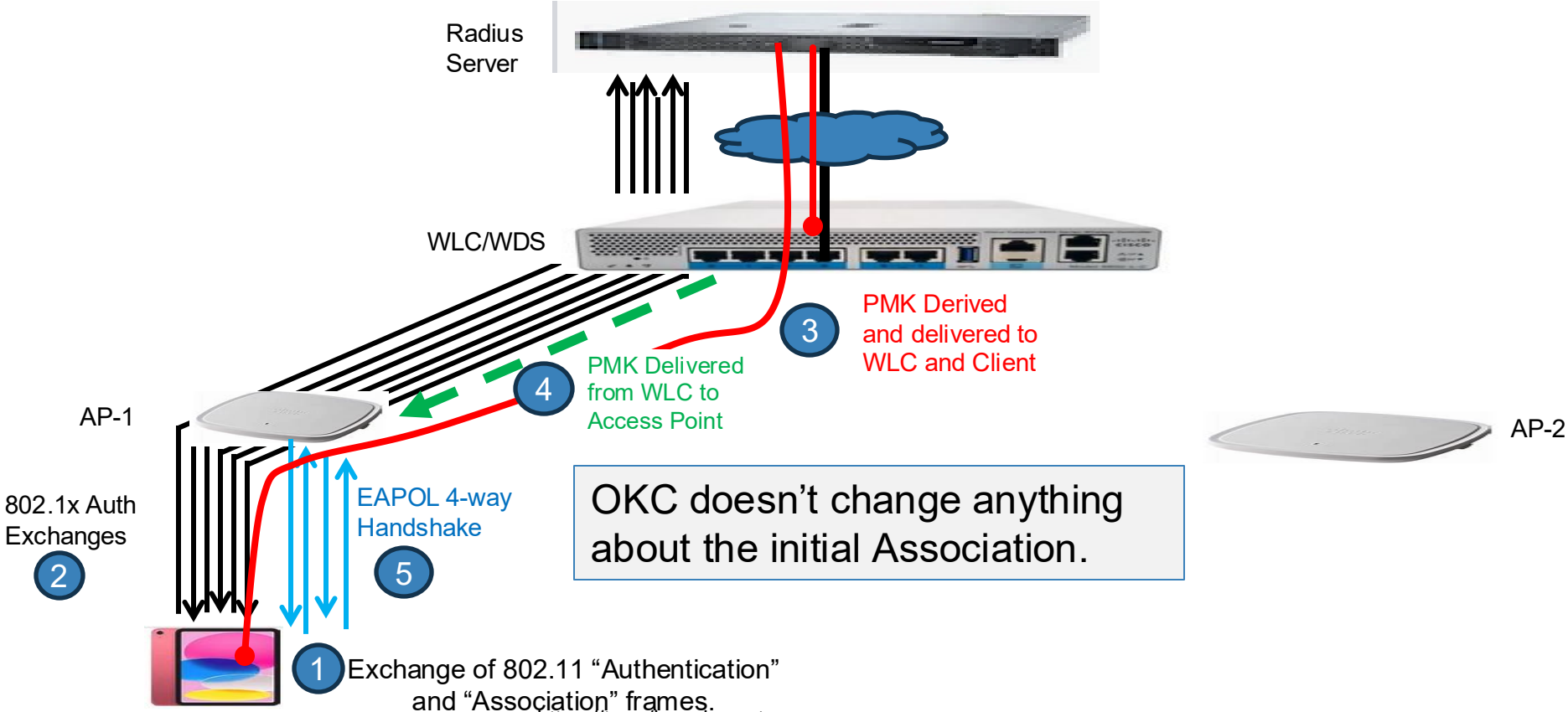
OKC Overview

- 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

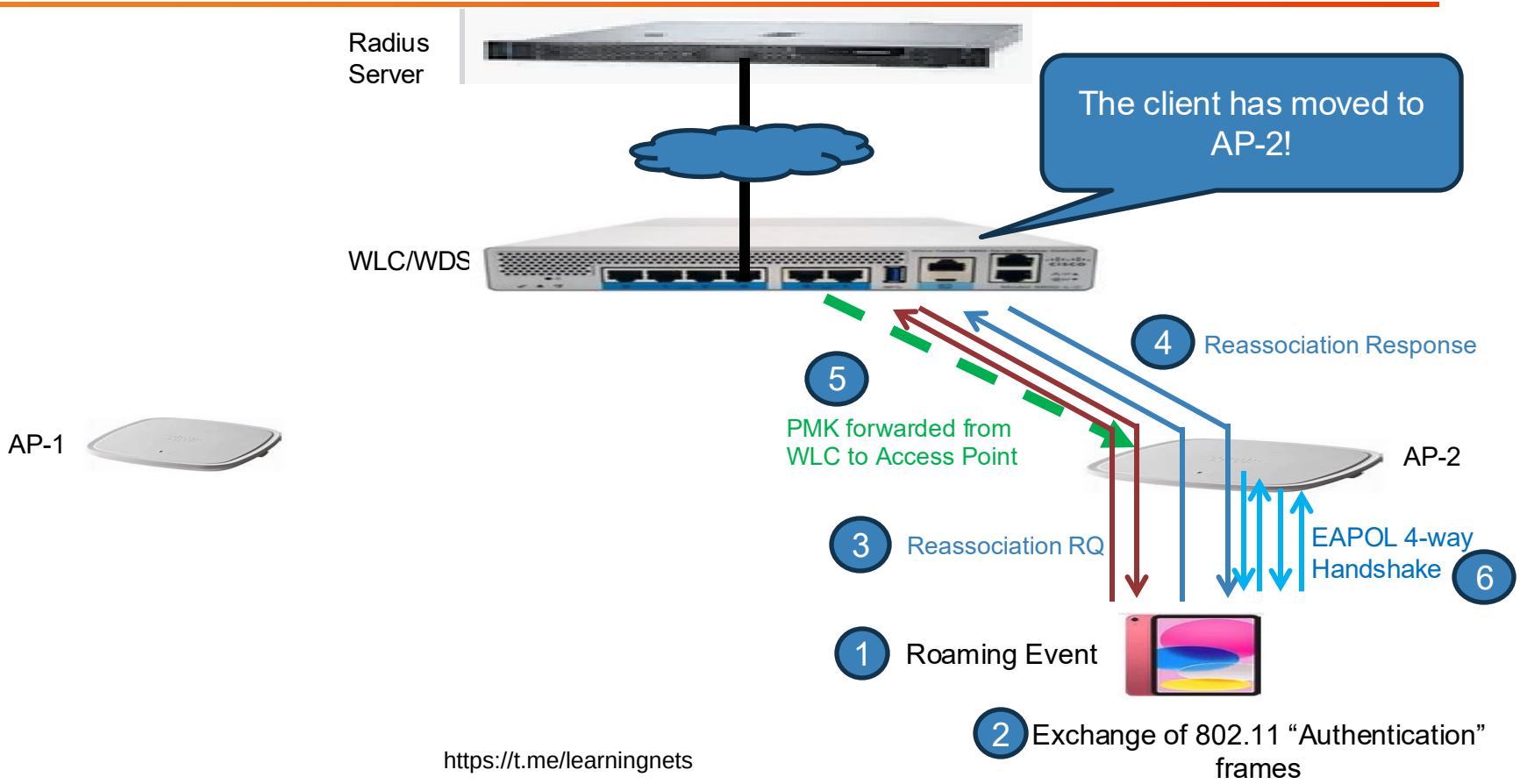
1. Client detects need to roam → decides on a new AP.
2. Client sends Reassociation Request to the target AP.
3. Target AP forwards the request to the WLC.
4. WLC checks its PMK cache (keyed by client MAC + SSID) to see if a valid PMK exists from a previous 802.1X authentication.
5. If PMK exists:
   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



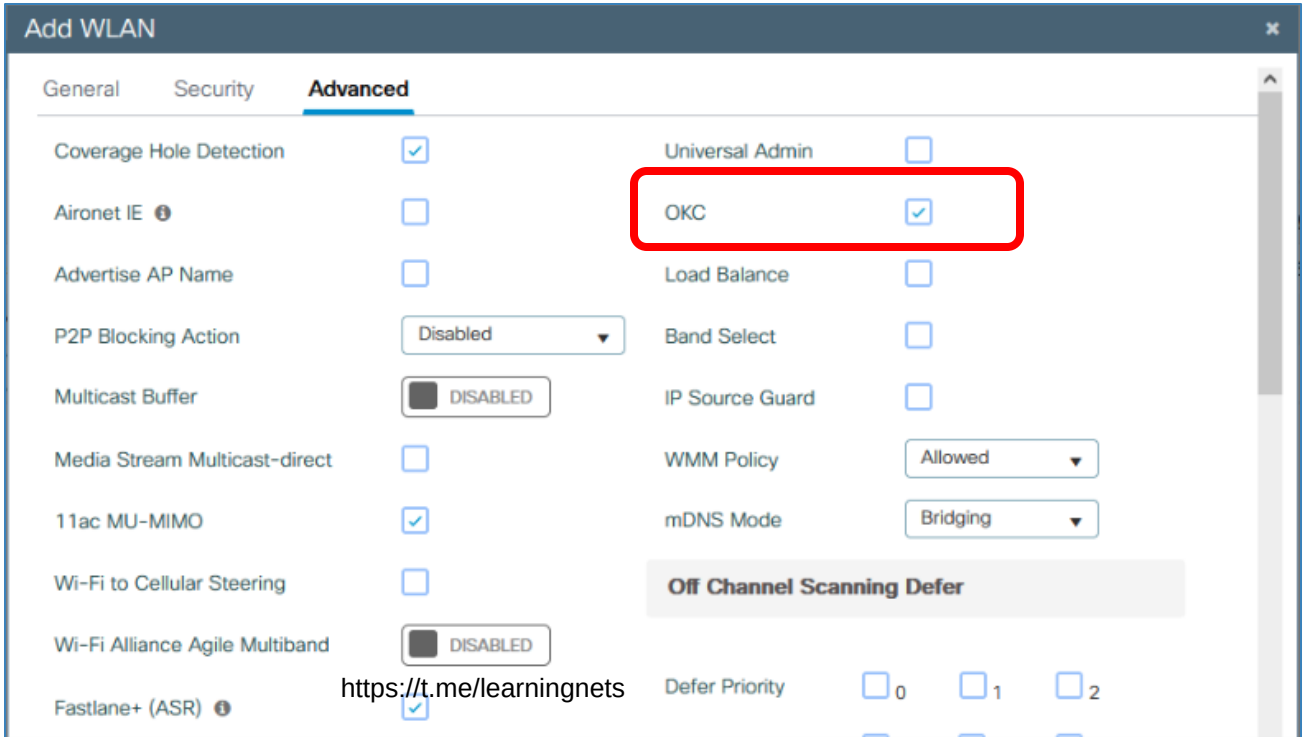
OKC doesn’t change anything about the initial Association.

Optimized Roaming with OKC



OKC Configuration

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



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)

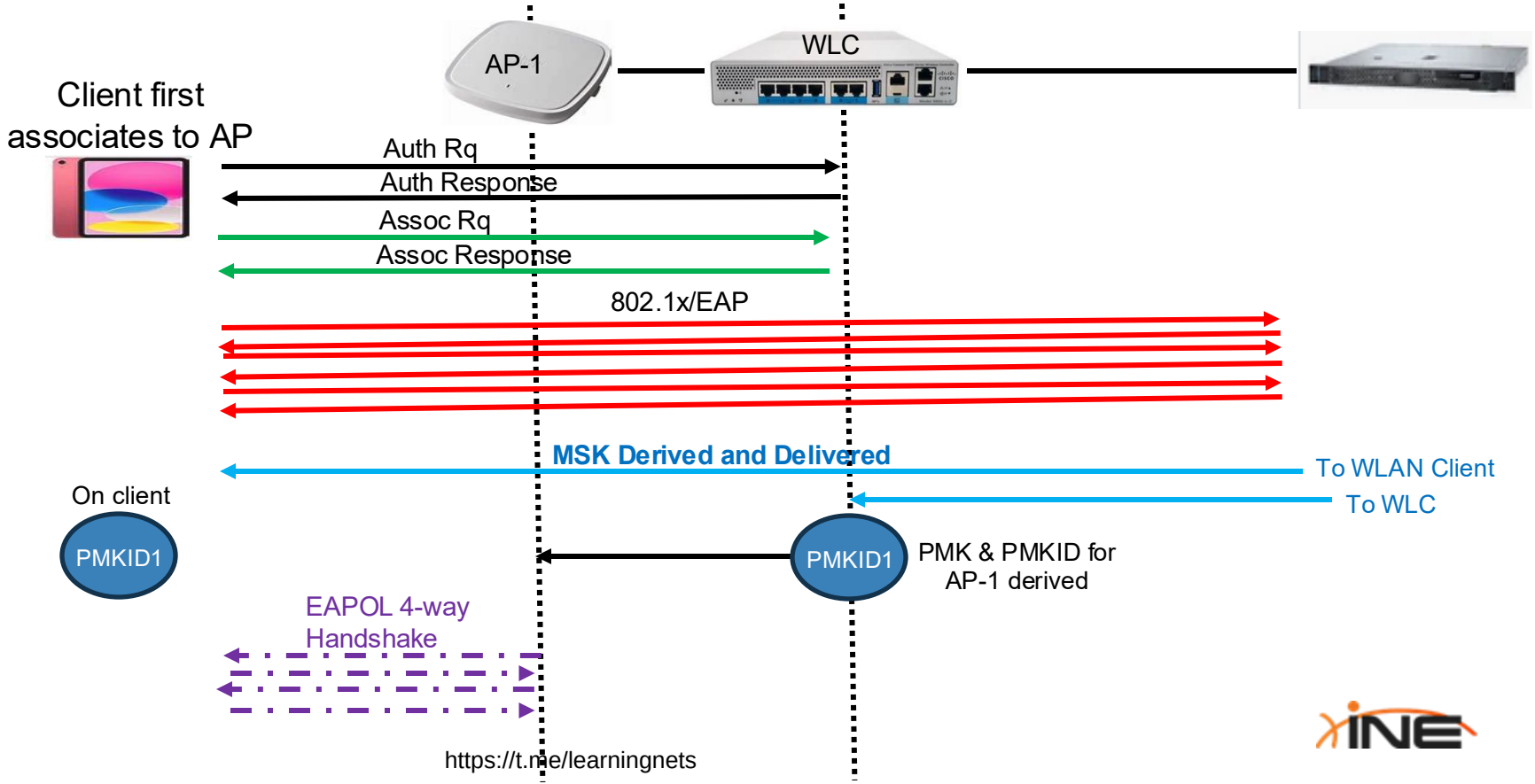
Thank you for watching!!

Sticky Key Caching

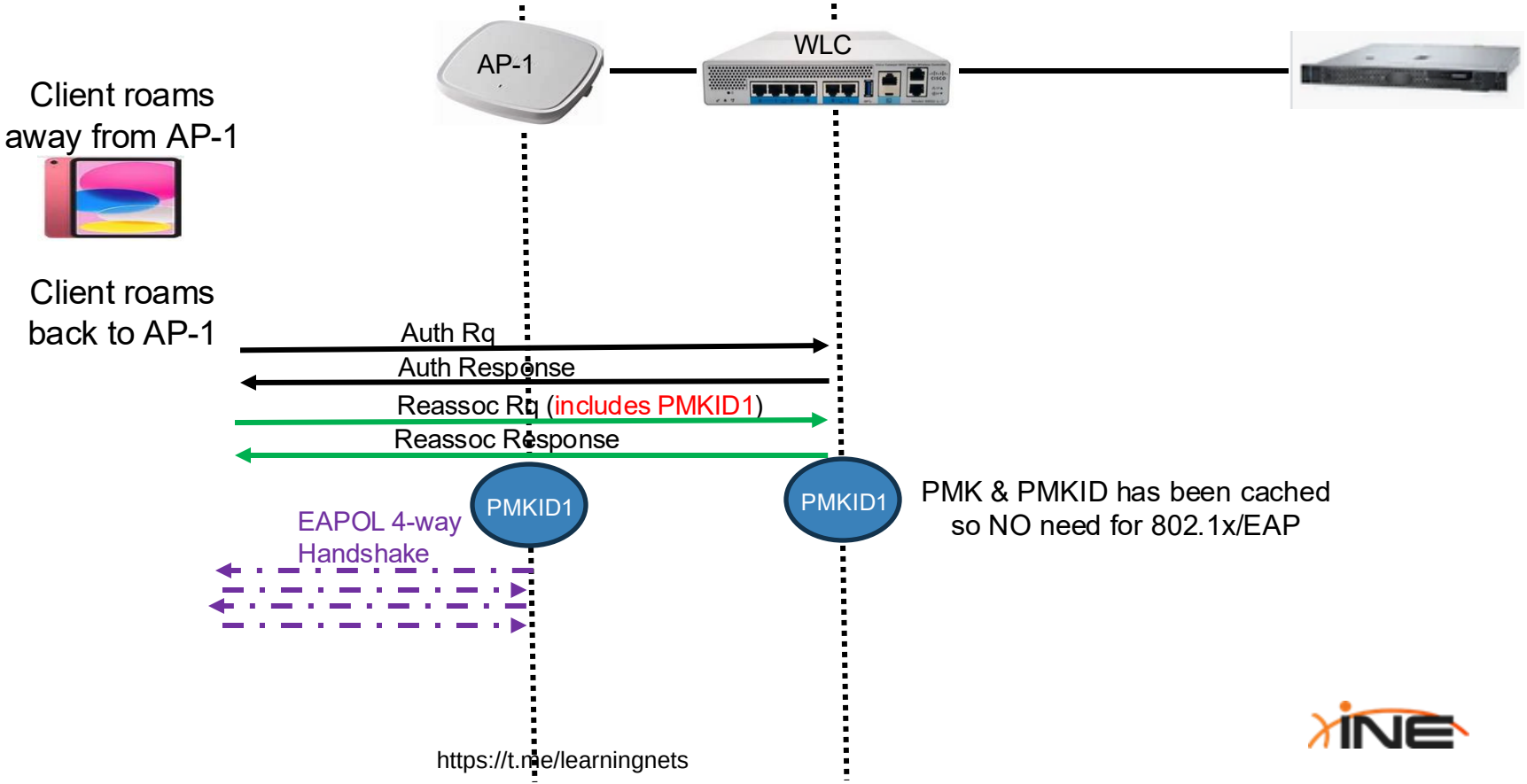
What Problem Did it Solve?

- 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)
```

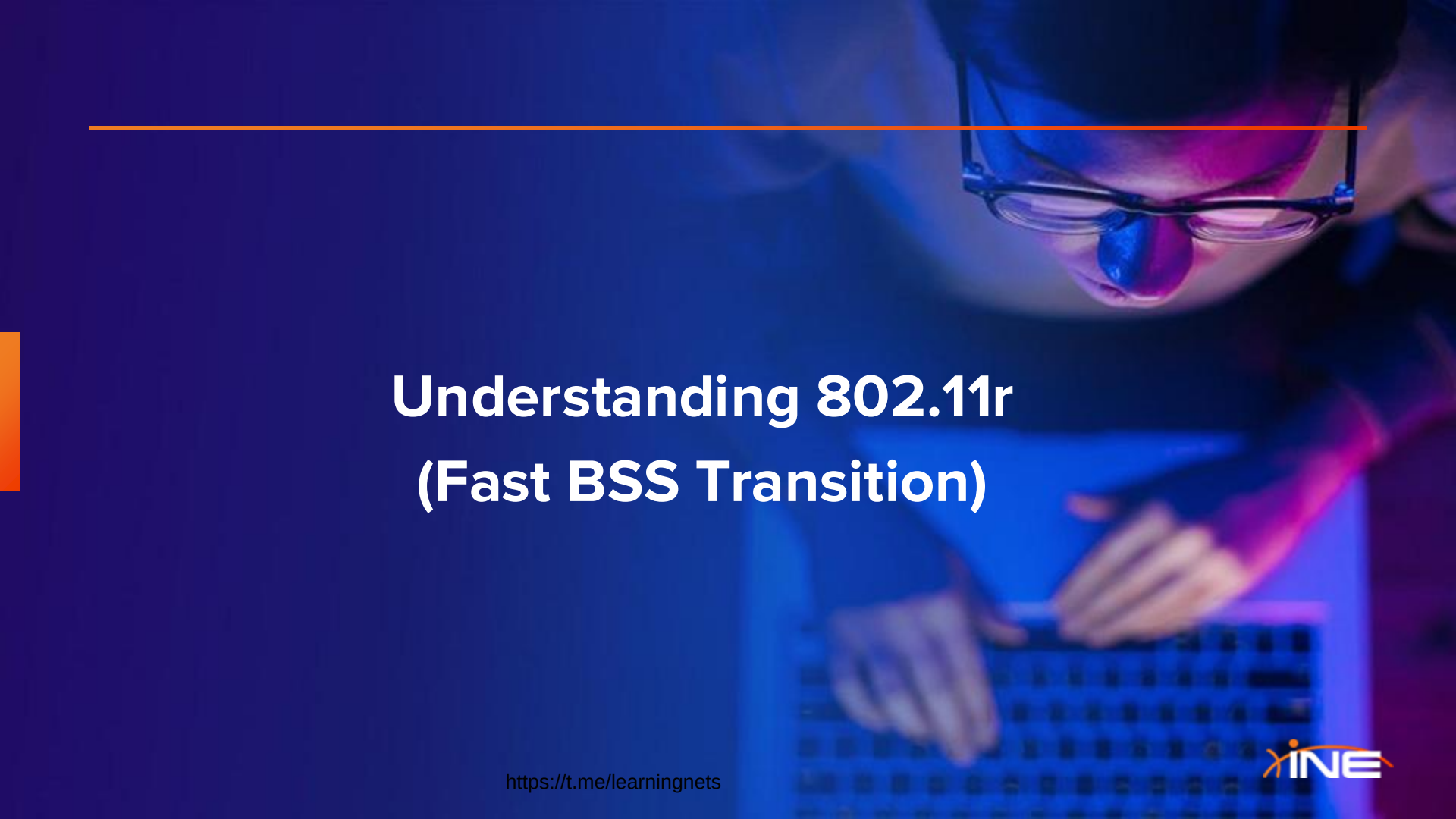
```
› Tag: SSID parameter set: "Dot1x-Test"
› Tag: Supported Rates 6(B), 9, 12(B), 18, 24(B), 36, 48, 54, [Mbit/sec]
› Tag: Power Capability Min: 8, Max: 23
› Tag: Supported Channels
⌄ Tag: RSN Information
    Tag Number: RSN Information (48)
    Tag length: 38
    RSN Version: 1
  › Group Cipher Suite: 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) 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: 0x0000
    PMKID Count: 1
  ⌄ 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)

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

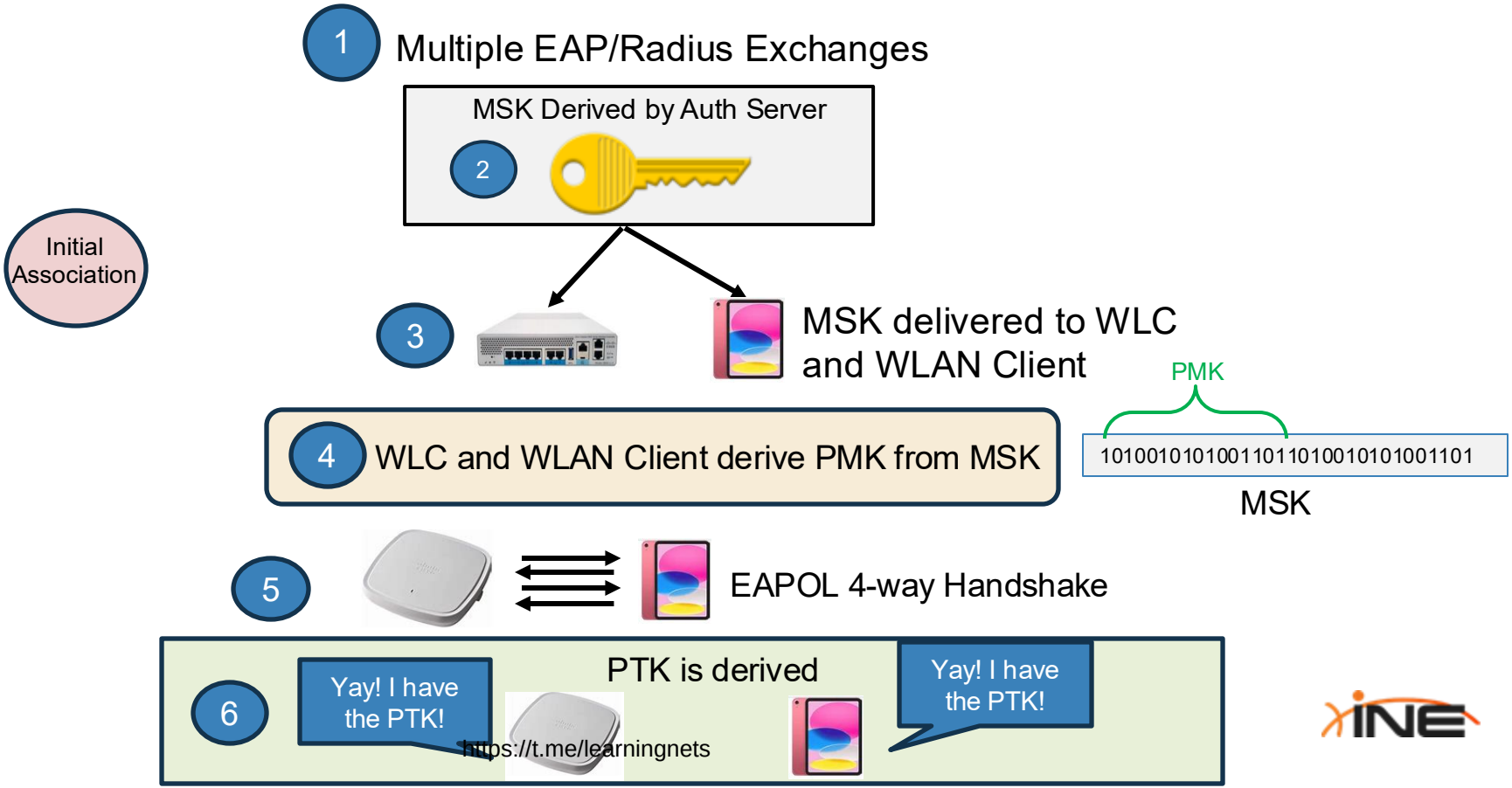
What is 802.11r (Fast BSS Transition)?

- 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

MSK Derived by Auth Server

2

Initial Association

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

3

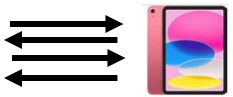
MSK delivered to WLC and WLAN Client

6

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

4 WLC and WLAN Client derive PMK-R0 from MSK

7

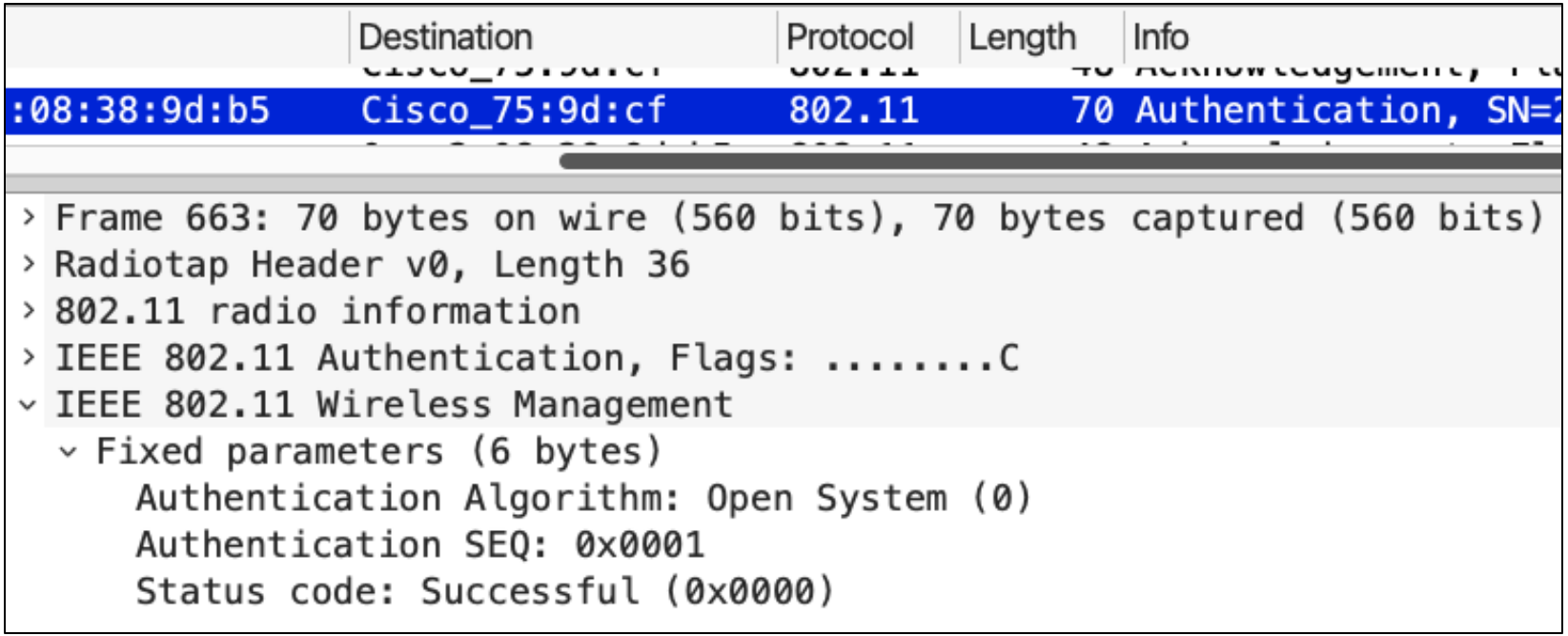


EAPOL 4-way Handshake using **PMKR1** derives PTK

Roaming with FT

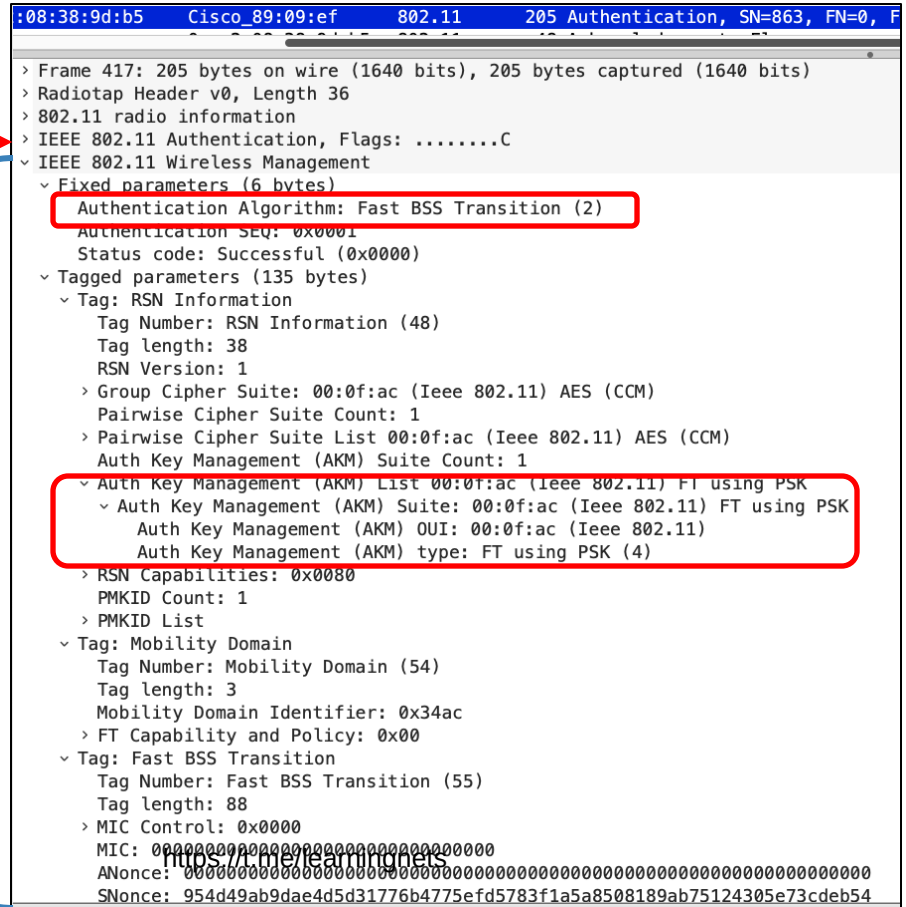
- When WLAN clients roam with 802.11r the 802.11 "Authentication" message is modified
- The new Authentication message includes;
  - "**Fast BSS Transition**" as "*authentication algorithm*"
  - "**Mobility Domain**" information
  - Various **nonces**
  - **PMK-R0 key holder** information
- This new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

802.11 Authentication Message w/o FT

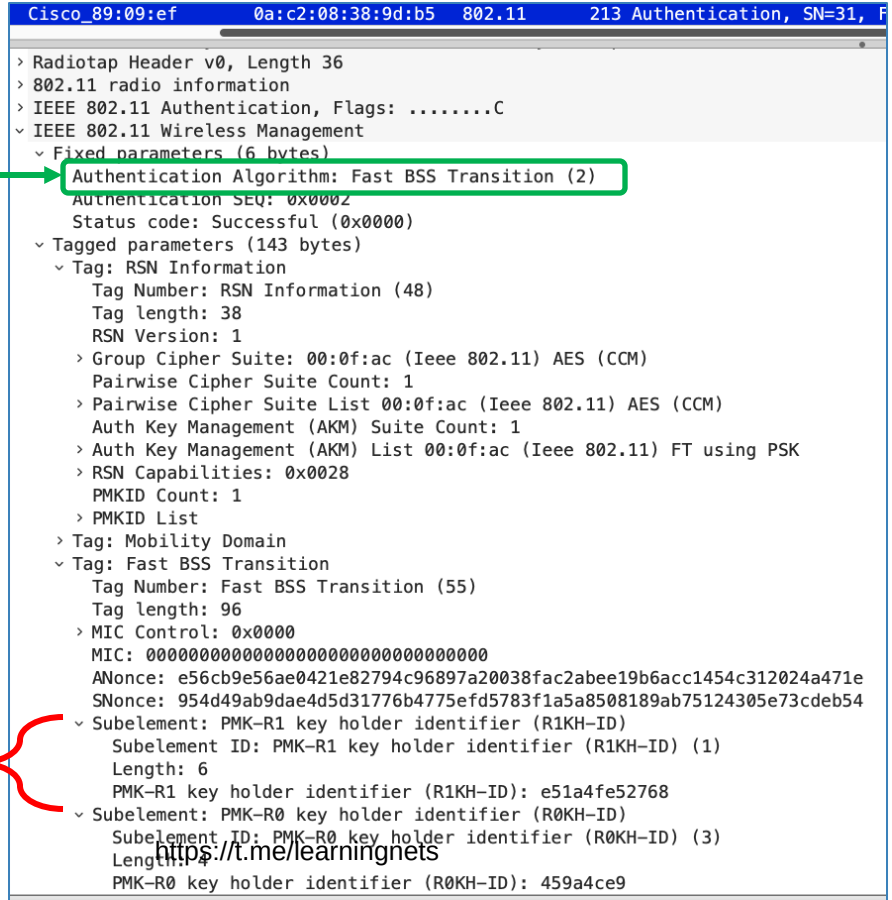


FT Request from WLAN Client

New Fields added by 802.11r (FT)

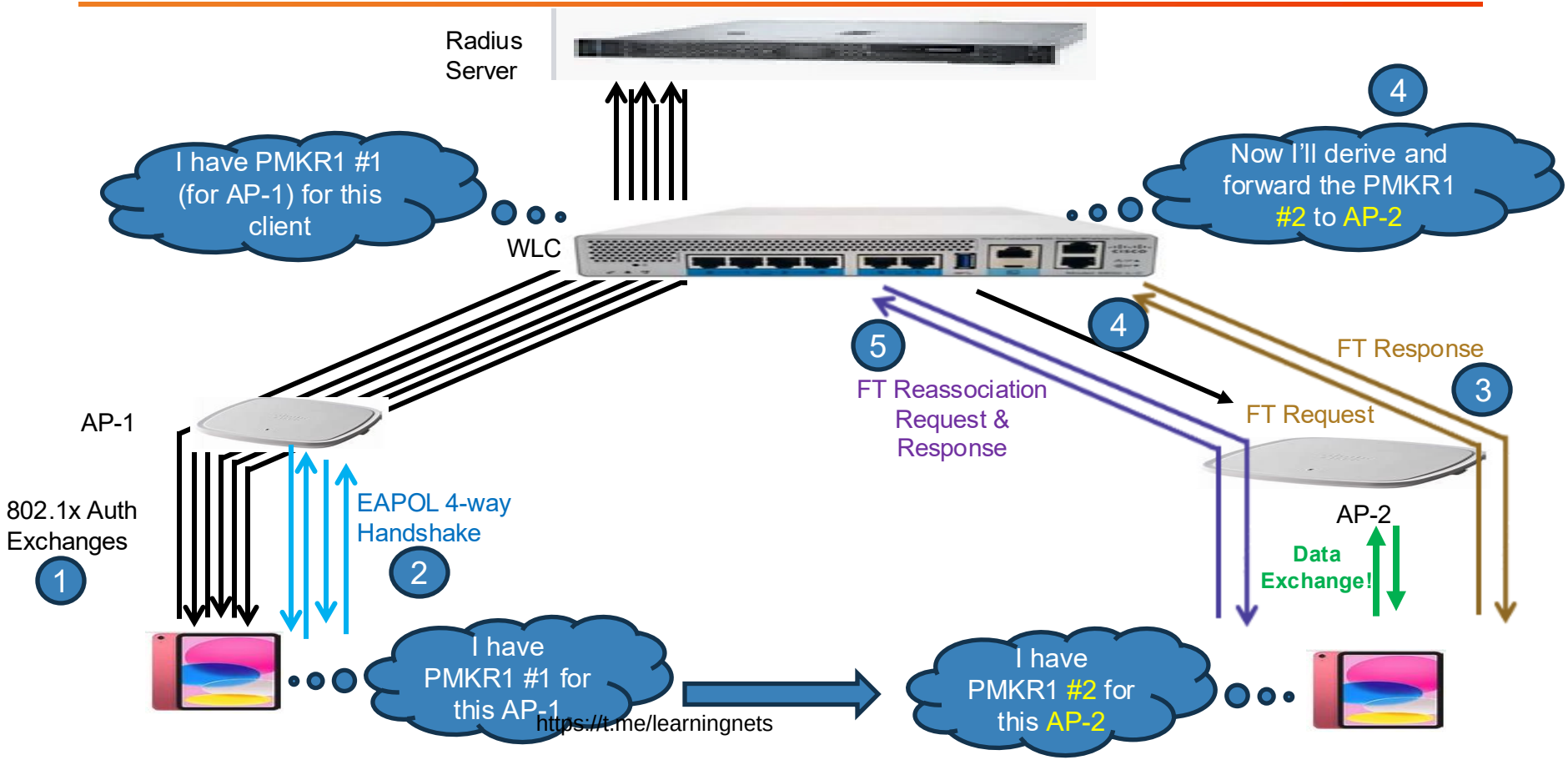


FT Response from Access Point

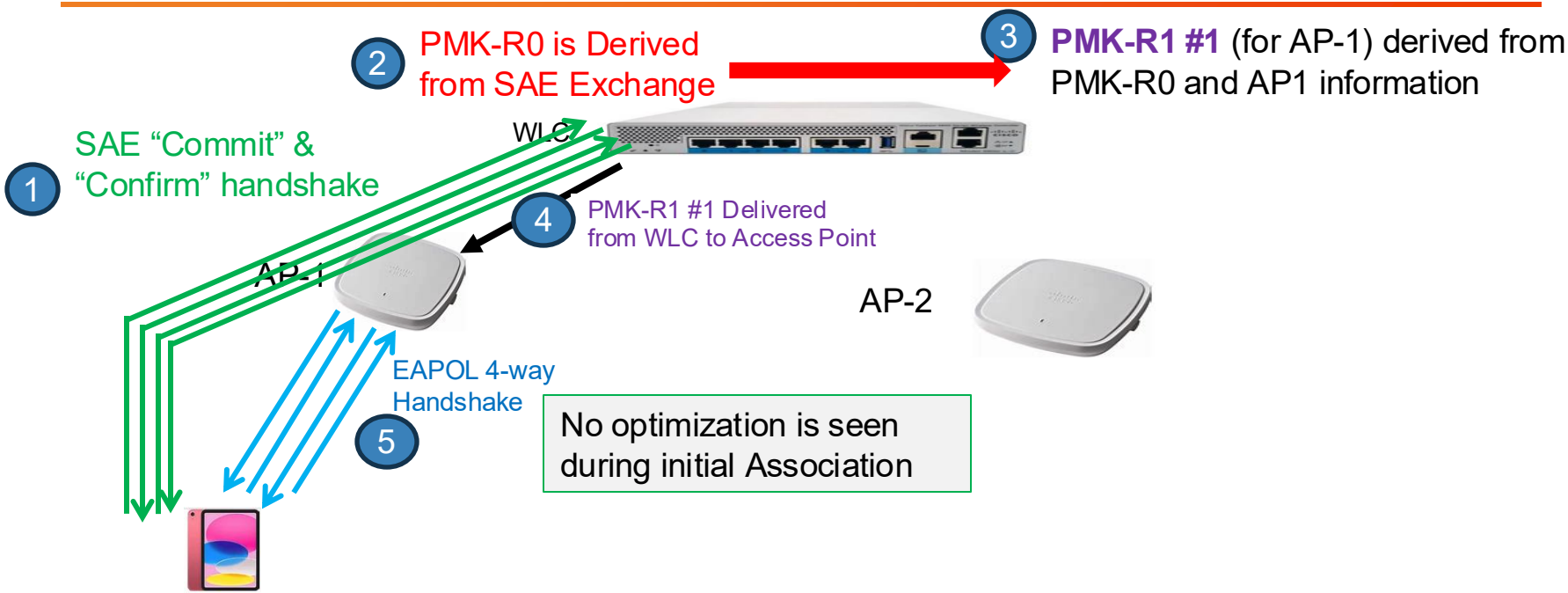


Notice the AP/WLC provides the PMK-R1 Key Holder ID

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.

802.11r Optimization with WPA Personal

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

3

Now I'll derive and forward PMKR1 #2 to AP-2

3

FT Response

2

FT Request

FT Reassociation Request & Response

4

AP-2

Data Exchange!

5

Client initiates roam event

1

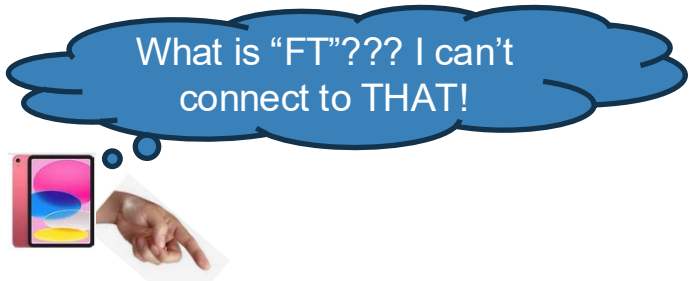
I can derive PMKR1 #2 for this AP-2

Thank you for watching!!

Fast Transition Modes

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

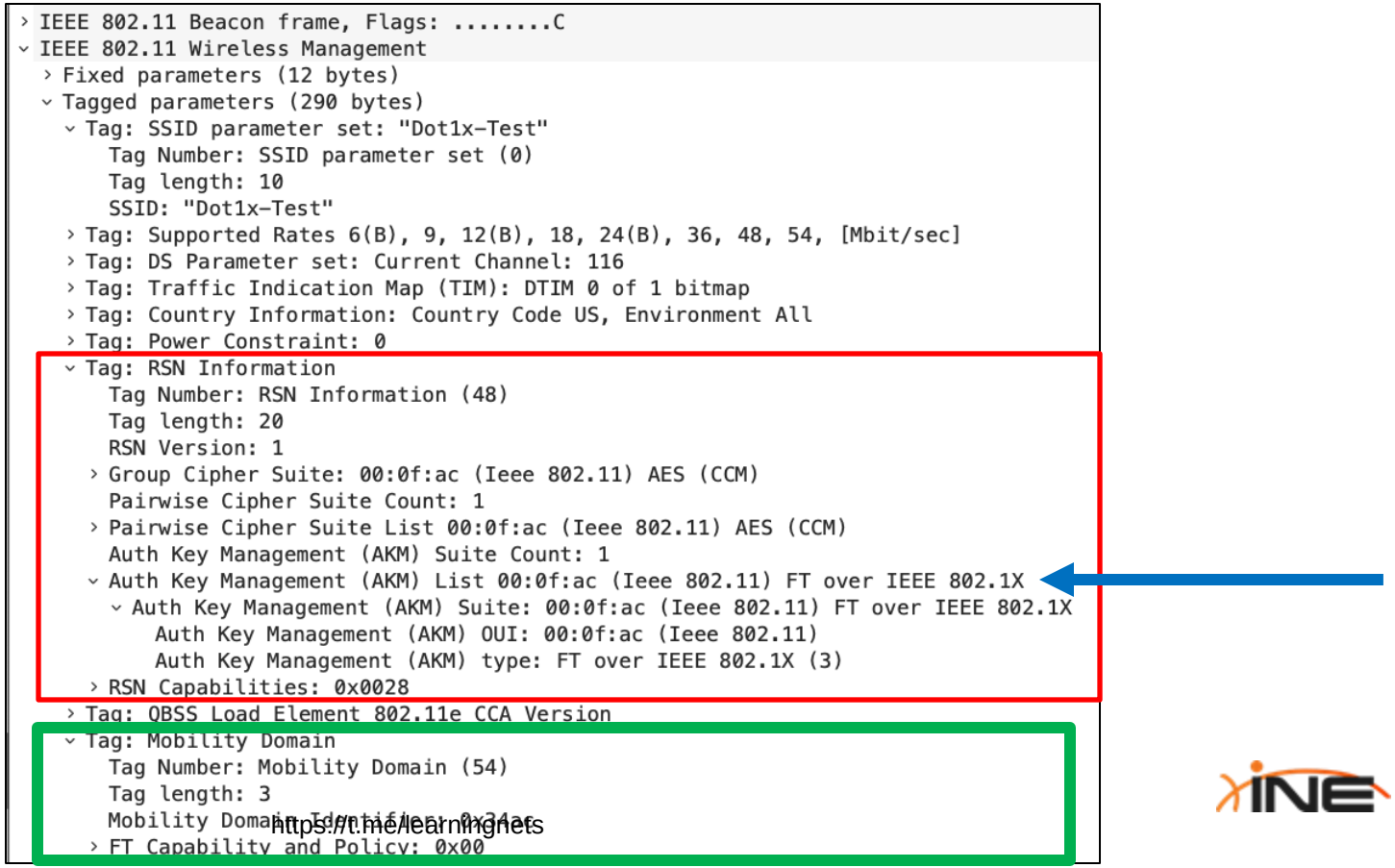



```
Auth Key Management (AKM) List 00:0f:ac (Ieee 802.11) FT over IEEE 802.1X
```

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

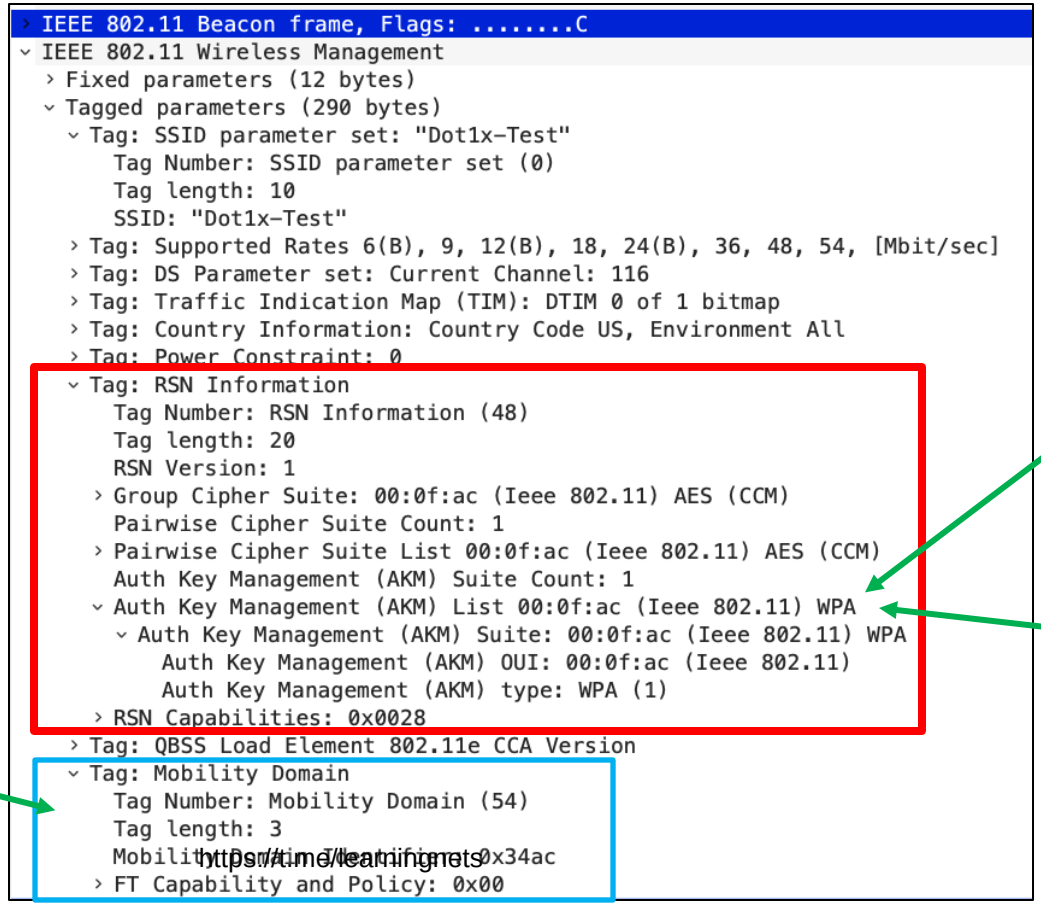
FT Only Mode



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)

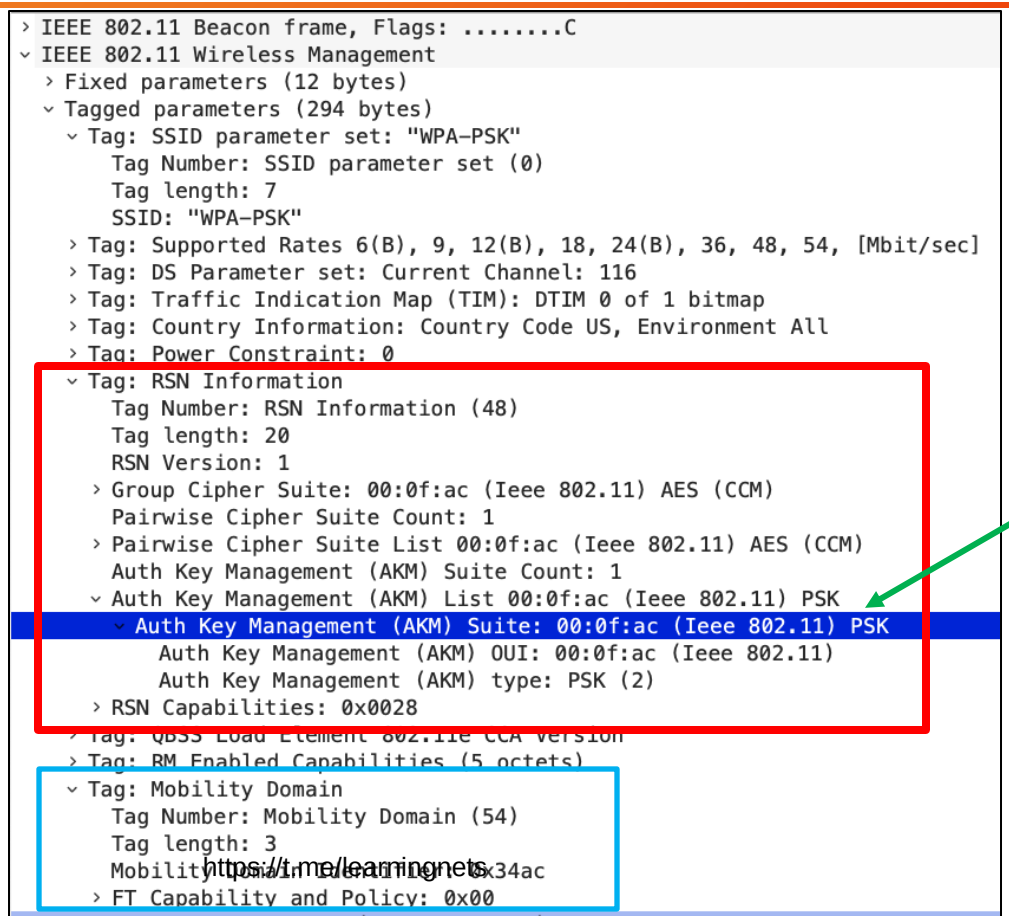


No mention of “FT” within AKM methods.

”WPA” displayed on WPA Enterprise WLANs

FT-capable clients will understand “Mobility Domain”

FT Adaptive Mode (Personal)

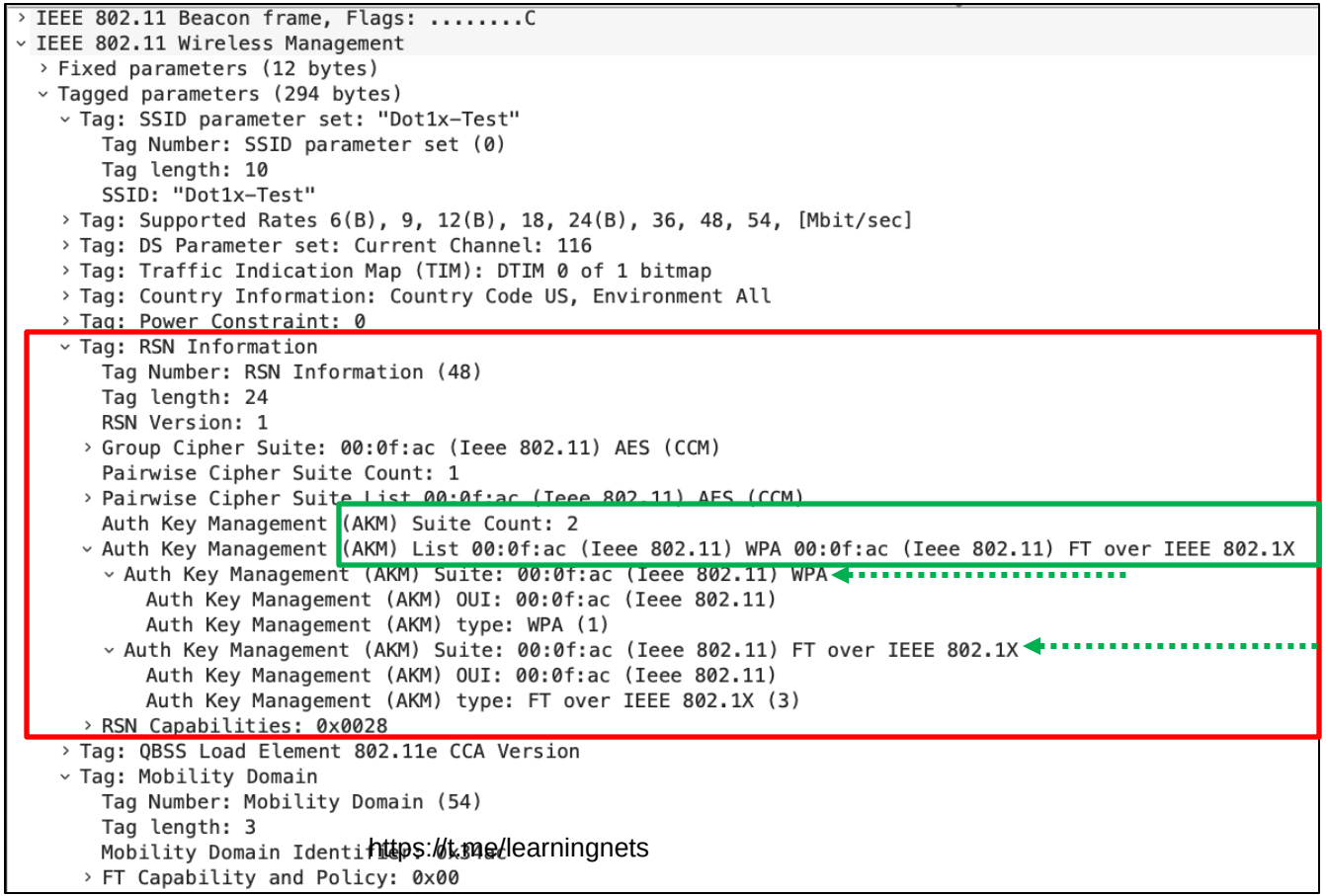


”PSK” displayed on WPA Personal WLANs

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



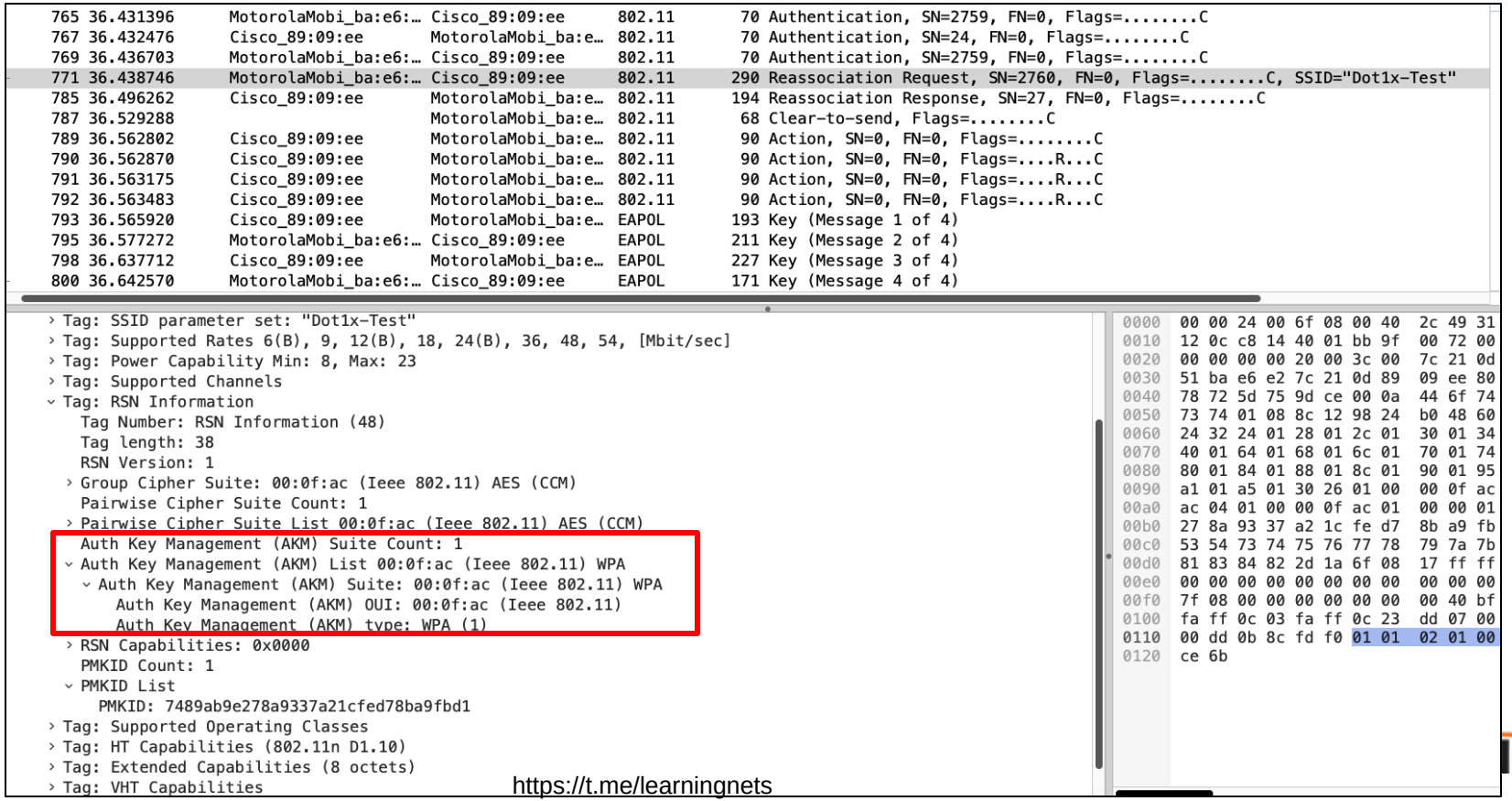
So What is Best?

From the document "Cisco Catalyst 9800 Series Configuration Best Practices"

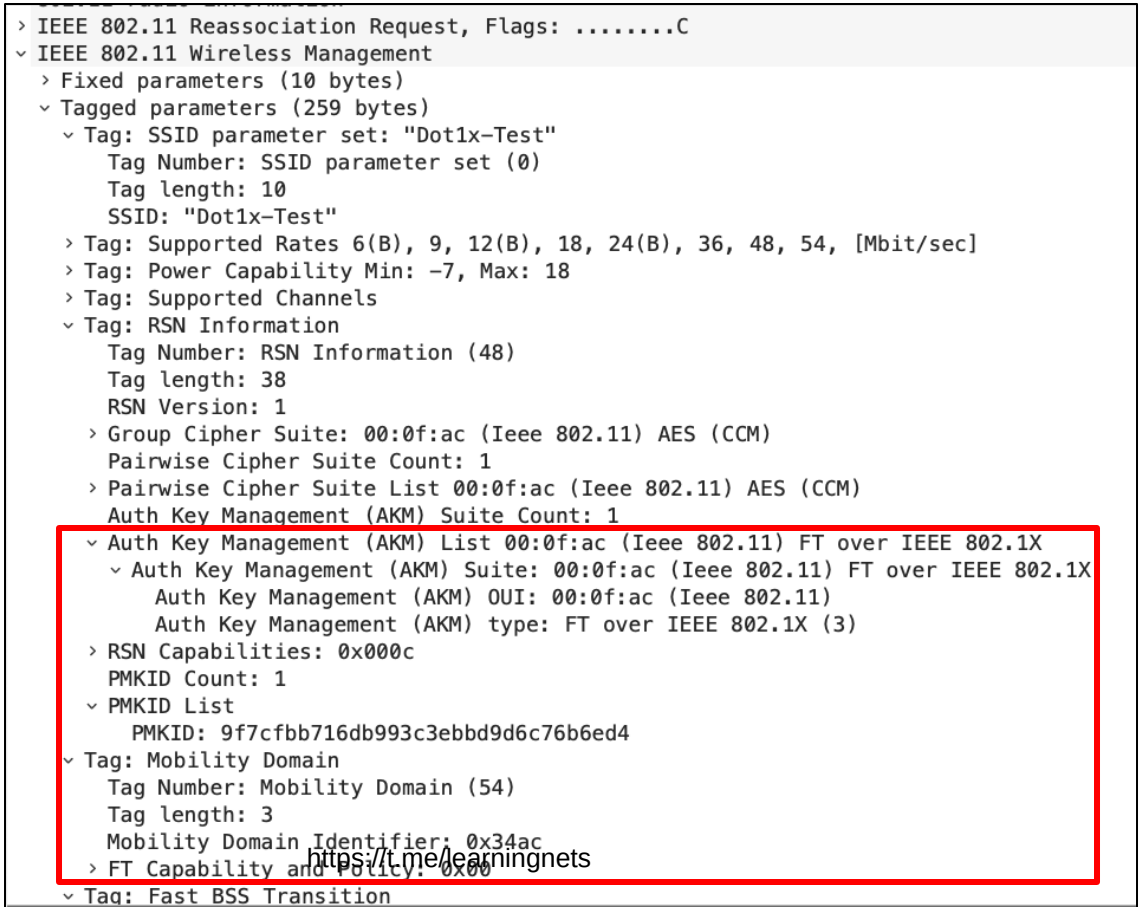
The reality is that in a mixed-client network, some non-FT clients may experience issues in connecting to a WLAN with Adaptive FT, so the recommendation from Cisco is to configure a single WLAN with "802.11r mixed mode", to allow for compatibility between 802.11r and non-802.11r clients

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



Adaptive Mode with Apple iPad

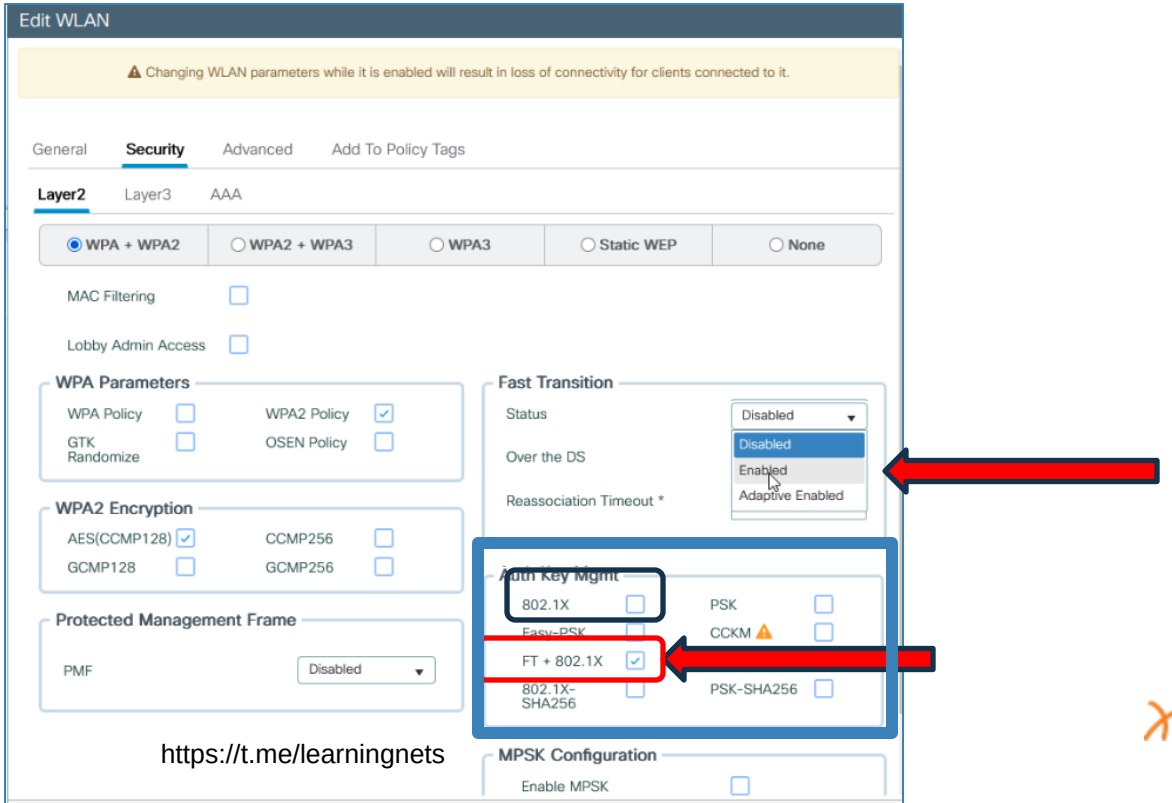


Thank you for watching!!

Configuring & Verifying Fast BSS Transition (802.11r)

Enabling 802.11r on the Catalyst 9800

- 802.11r is typically enabled by default, but if not…



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

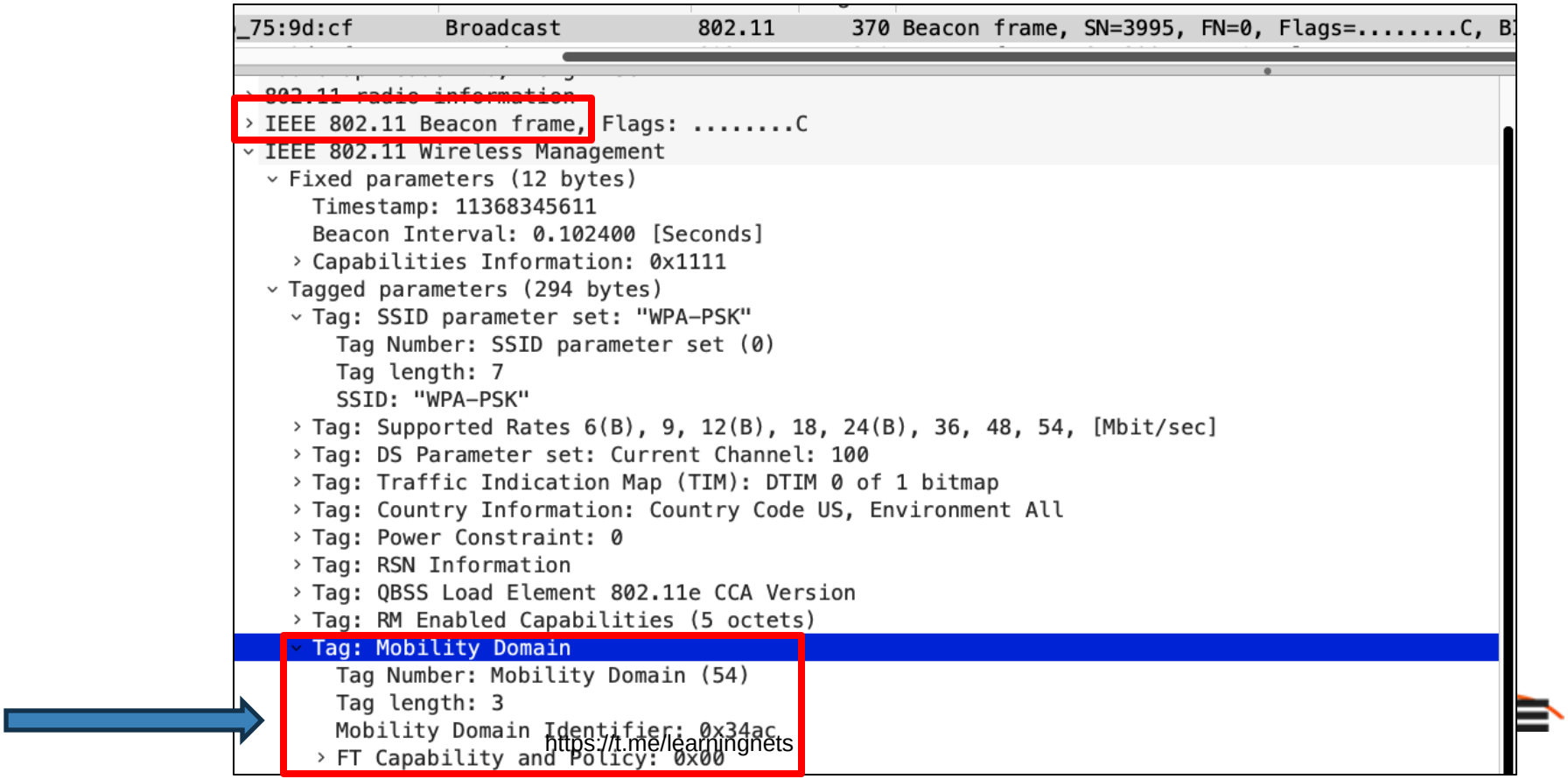
Full Radius/EAP Exchange

Packet Capture: 802.11r Roam

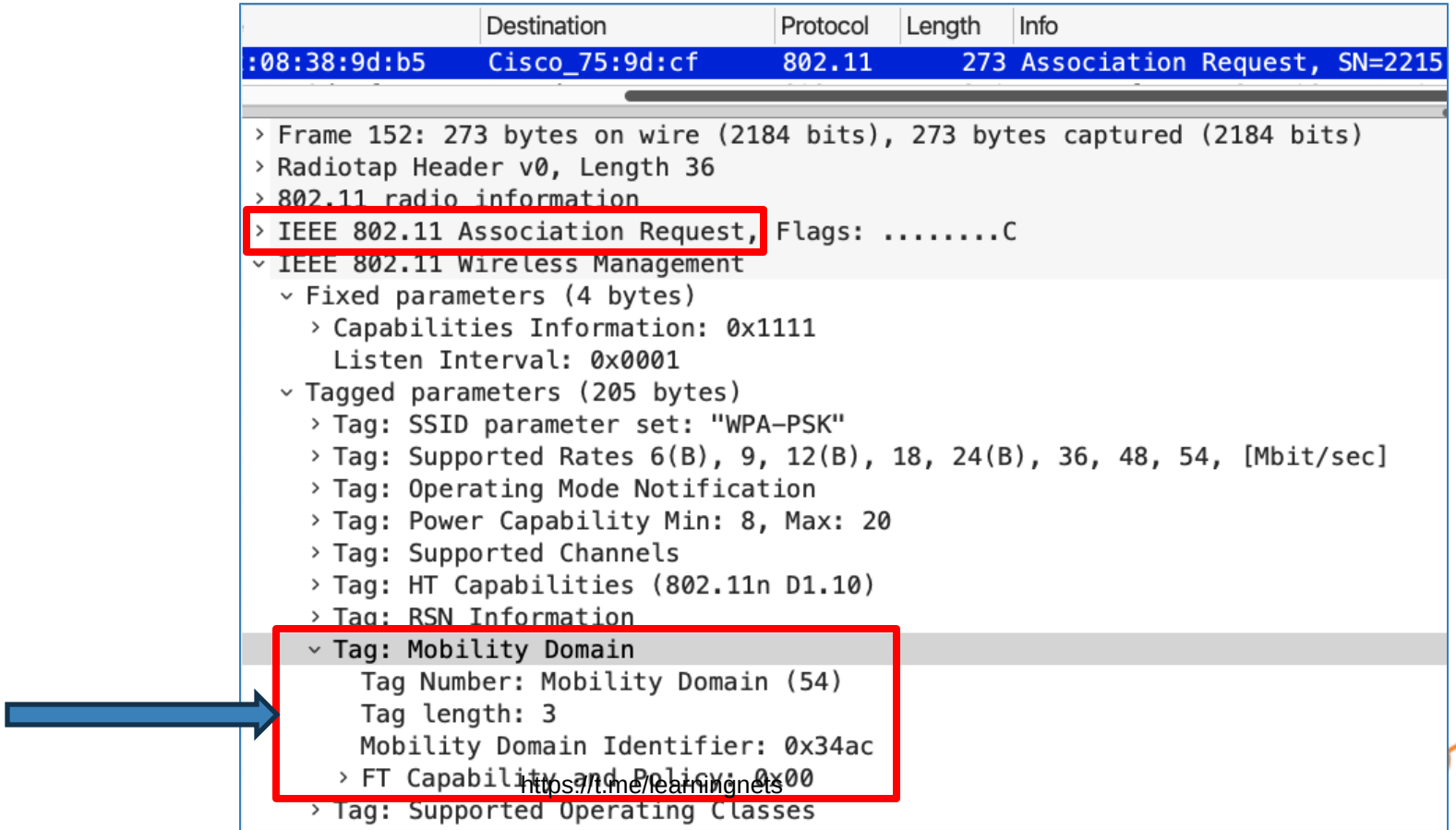
Source	Destination	Protocol	Length	Info
da:ff:ce:28:22:b8	Cisco_89:09:ee	802.11	205	Authentication, SN=3555, FN=0, Flags=........C
Cisco_89:09:ee	da:ff:ce:28:22:b8	802.11	213	Authentication, SN=876, FN=0, Flags=........C
da:ff:ce:28:22:b8	Cisco_89:09:ee	802.11	439	Reassociation Request, SN=3556, FN=0, 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



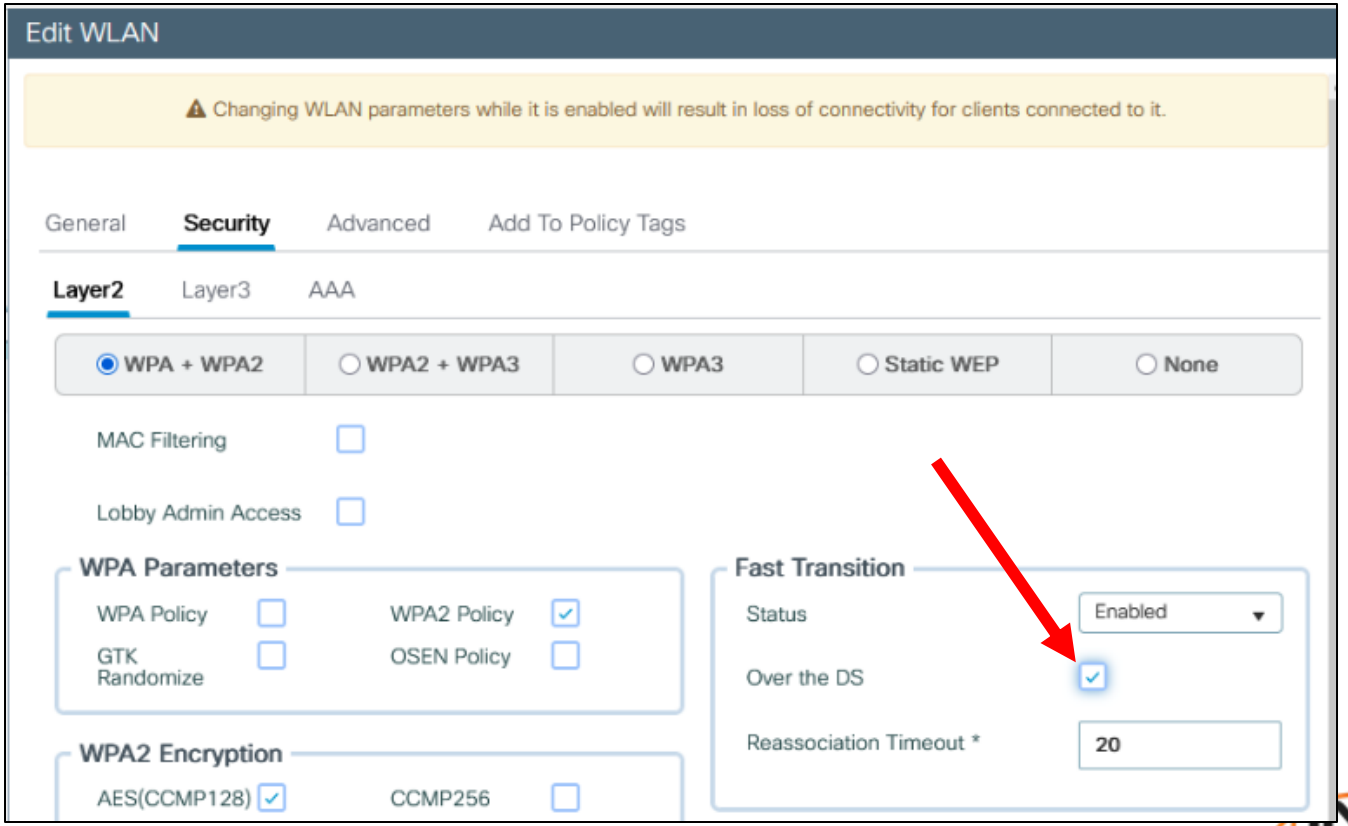
Verifying Client Support for 802.11r



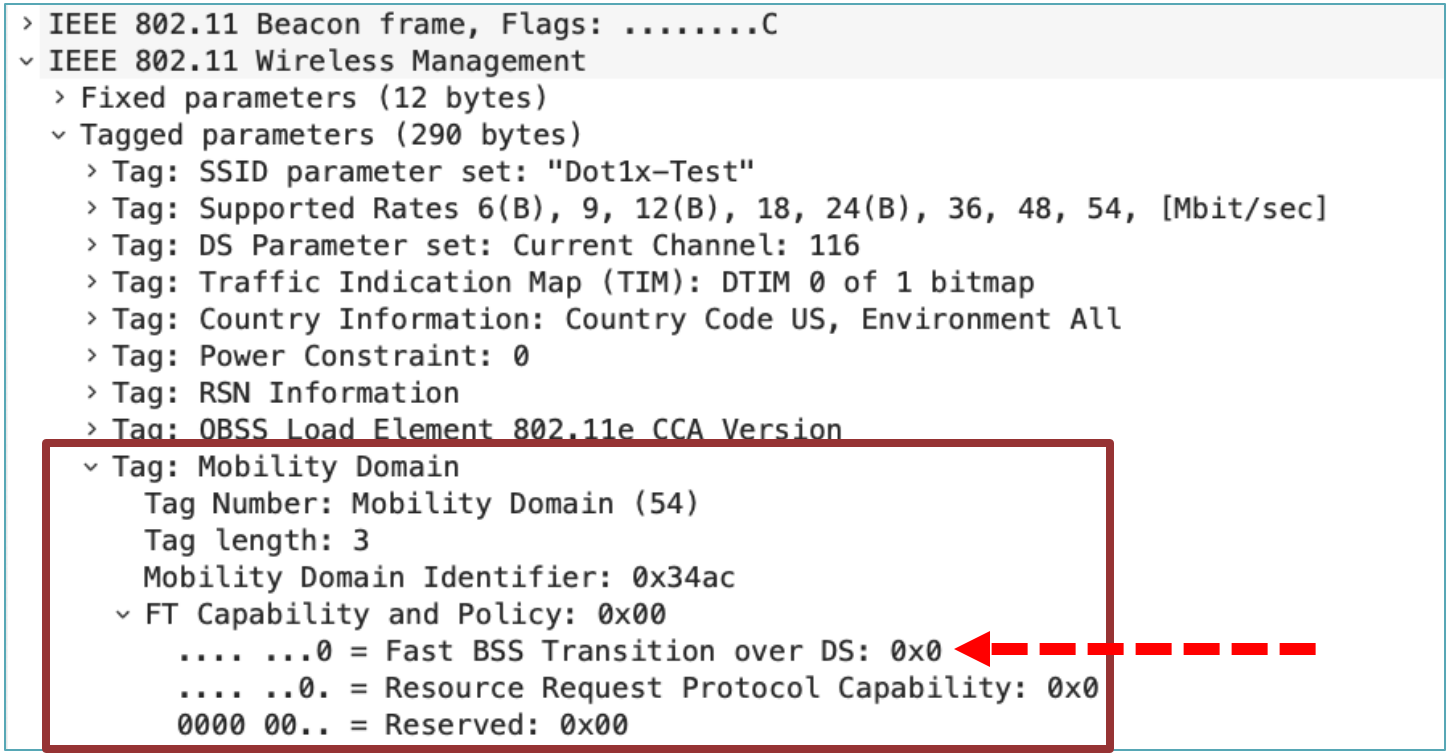
Over-The-DS

- 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.

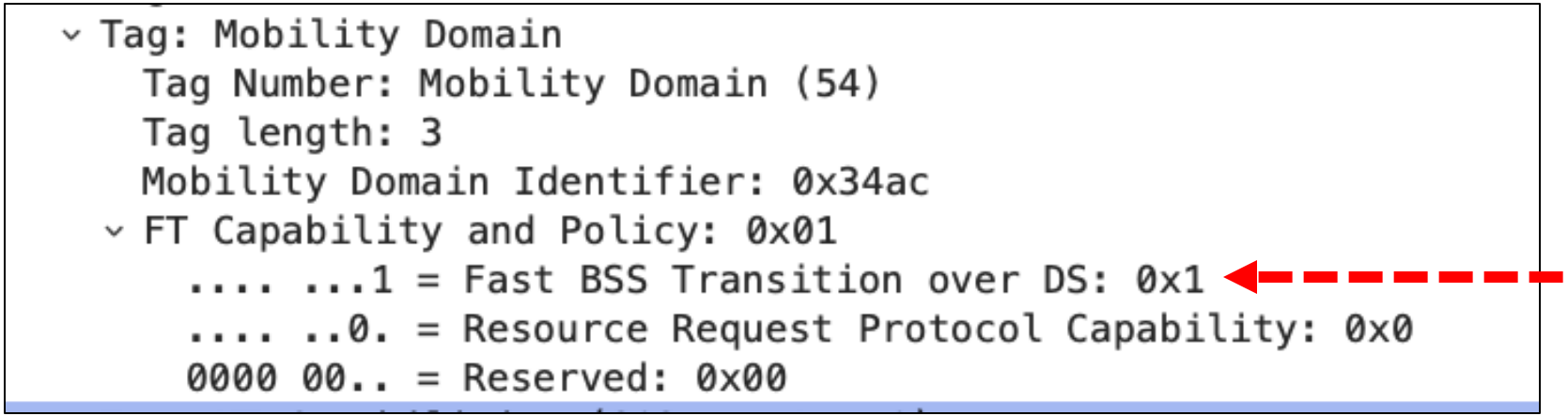
Over-the-DS Configuration



FT with Over-the-Air



Over-the-DS Verification



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

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!

EXPERTS AT MAKING YOU AN EXPERT