

The background features a vibrant, abstract design with a color gradient from dark blue on the left to bright yellow and white on the right. The design consists of overlapping, wavy horizontal bands and a radial pattern of lines emanating from a bright white point on the right side, creating a sense of motion and energy.

CISCO *Live!*

Let's go



The bridge to possible

# Understanding Wireless Security

And the Implications for Secure Wireless Network Design

Mark Krischer, Principal Wireless Architect  
Asia Pacific, Japan & Greater China

# Agenda

- Wireless Security Fundamentals
  - WPA3
  - Authentication and Authorisation
  - Implications of 6GHz
- Rogue Detection and Advanced WIPS
  - Rogue Detection and Containment
  - Advanced Wireless Intrusion Prevention
- Network as a Sensor and Enforcer



# Wireless Security Fundamentals

# Securing the Wireless Network



Secure the  
Air



Secure the  
Devices



Secure the  
Network

“For Carlsberg,  
networking and security operations  
are ultimately about the same thing...  
*ensuring the beer keeps flowing.*”

Tal Arad, CISO and Head of Technology, Carlsberg

“Networking and security teams tasked to converge, collaborate”, NetworkWorld

# Wireless Attack Surface

- Wireless networks propagate beyond the physical constraints of the wired network
- Attacks may originate from anywhere within the wireless coverage
  - Passive scanning attacks
  - Layer 2 active spoofing attacks
  - Layer 1 active jamming or DoS attacks
  - Rogue APs
    - Honeypot and Evil Twin APs
    - Unsecured backdoor access

# Wireless Protected Access

## WPA

- A snapshot of the 802.11i Wireless Security Standard
- Commonly used with TKIP encryption

## WPA2

- Final version of 802.11i Wireless Security Standard
- Commonly used with AES encryption

## Authentication Mechanisms

- Personal (PSK – Pre-Shared Key)
- Enterprise (802.1X/EAP)

## WPA3

- Wi-Fi Alliance security update
- Includes new capabilities and new certification requirements



# WPA3

- Mandatory for Wi-Fi 6 Certification
- Remove insecure legacy protocols
  - WEP
  - TKIP
  - SHA1
- Negative Testing
  - KRACK
- Protected Management Frames (802.11w)
- Simultaneous Authentication of Equals (SAE)
- Wi-Fi Certified Enhanced Open
  - Opportunistic Wireless Encryption (OWE)

# 802.11 Fundamentals

## Authentication



# 802.11 Fundamentals

## Authentication



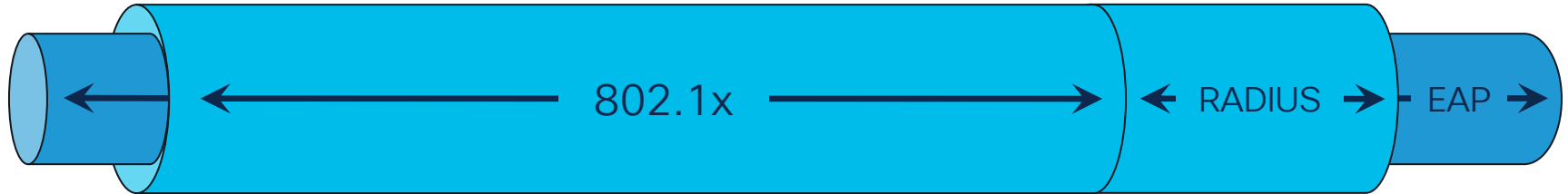
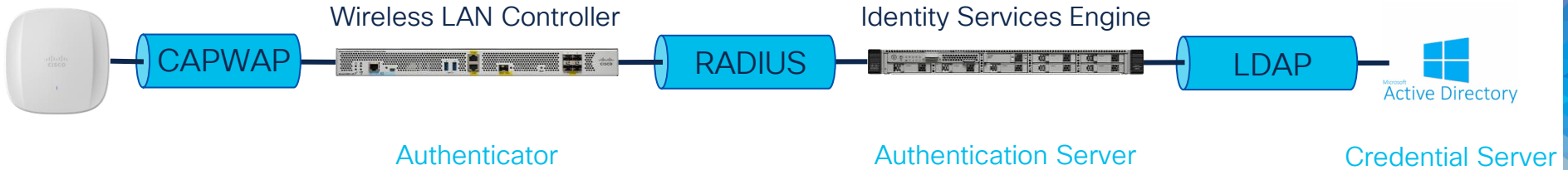
# 802.11 Fundamentals

## Authentication



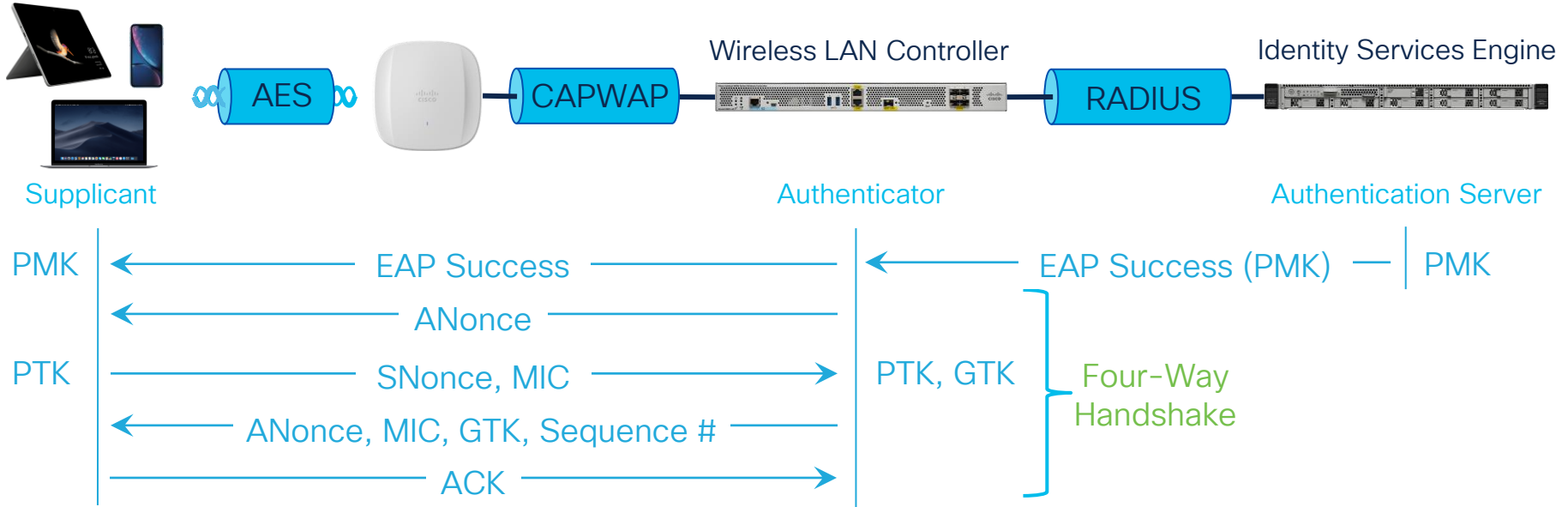
# 802.11 Fundamentals

## Authentication



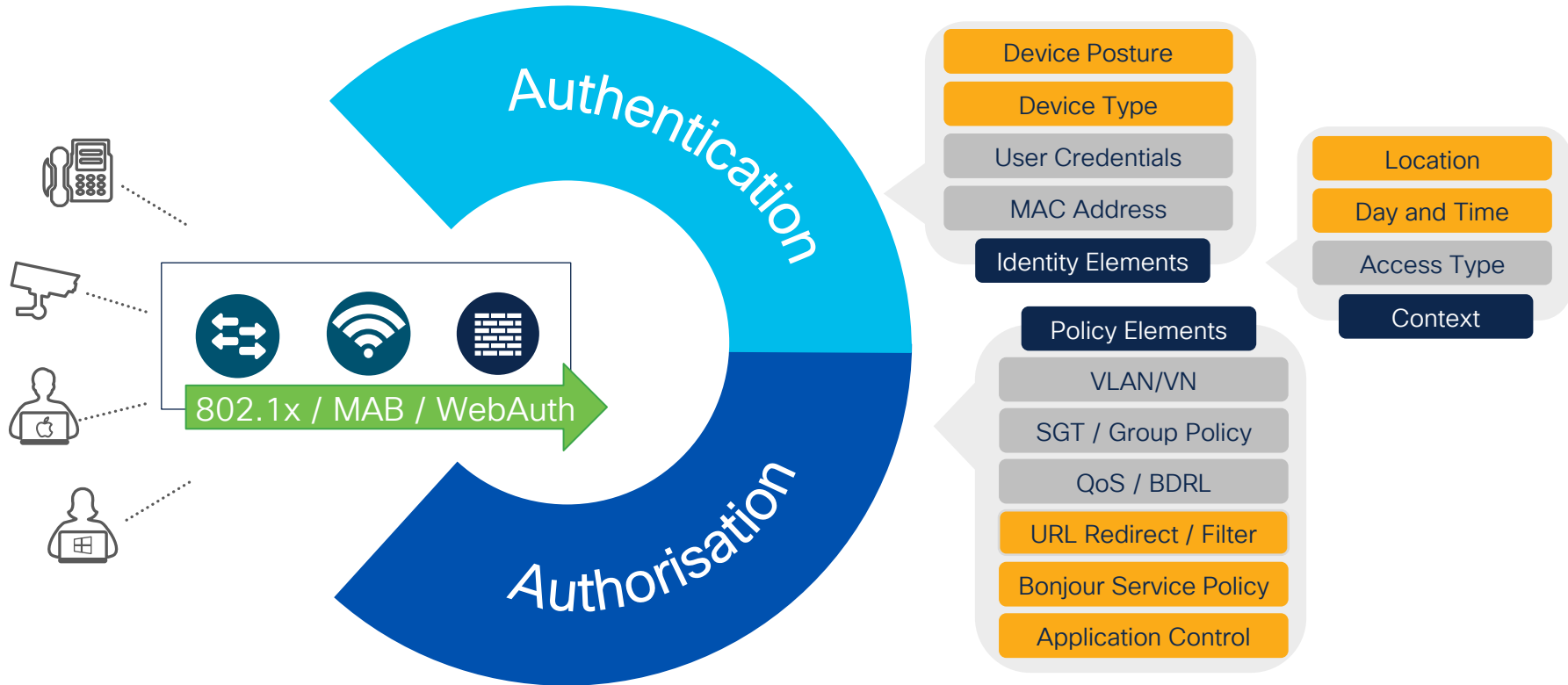
# 802.11 Fundamentals

## Encryption



$$PTK = \text{SHA}(\text{PMK} + \text{ANonce} + \text{SNonce} + \text{AP MAC} + \text{STA MAC})$$

# Authentication and Authorisation



# Authorisation

## Network Segmentation

### Static VLAN Assignment

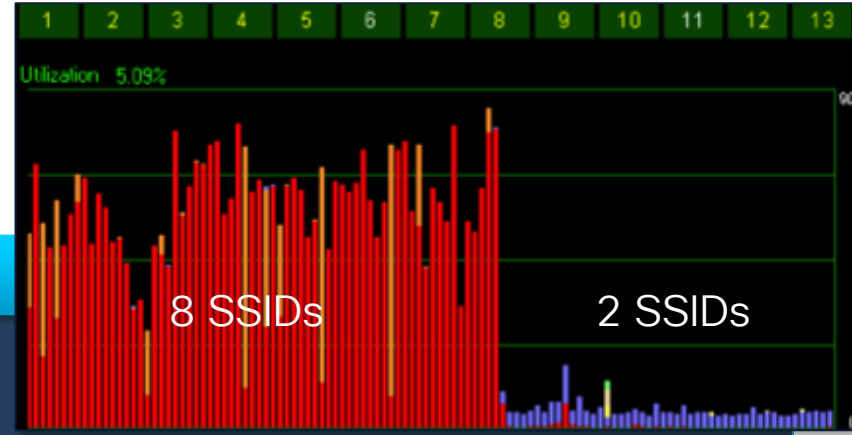
- VLAN based on SSID
- VLAN segregation based on security policy

### Dynamic VLAN Assignment

- VLAN based on authentication credentials
- VLAN segregation based on role

### TrustSec / Adaptive Policy / Software Defined Access

- Security based on TrustSec Scalable Group Tags instead of source and destination addresses
- ACLs applied at the packet level with enforcement across the network (or network fabric)





# Secure Fast Roaming Challenges



- Client channel scanning and AP selection
- Re-authentication of client device and re-keying

# Secure Fast Roaming

802.11k/v/r and Wi-Fi Agile Multiband



- Client channel scanning and AP selection
  - 802.11k Neighbor Lists based on CCX (Cisco Compatible Extensions)
  - 802.11v BSS Transition
- Re-authentication of client device and re-keying
  - 802.11r Fast BSS Transition based on CCKM (Cisco Centralised Key Management)



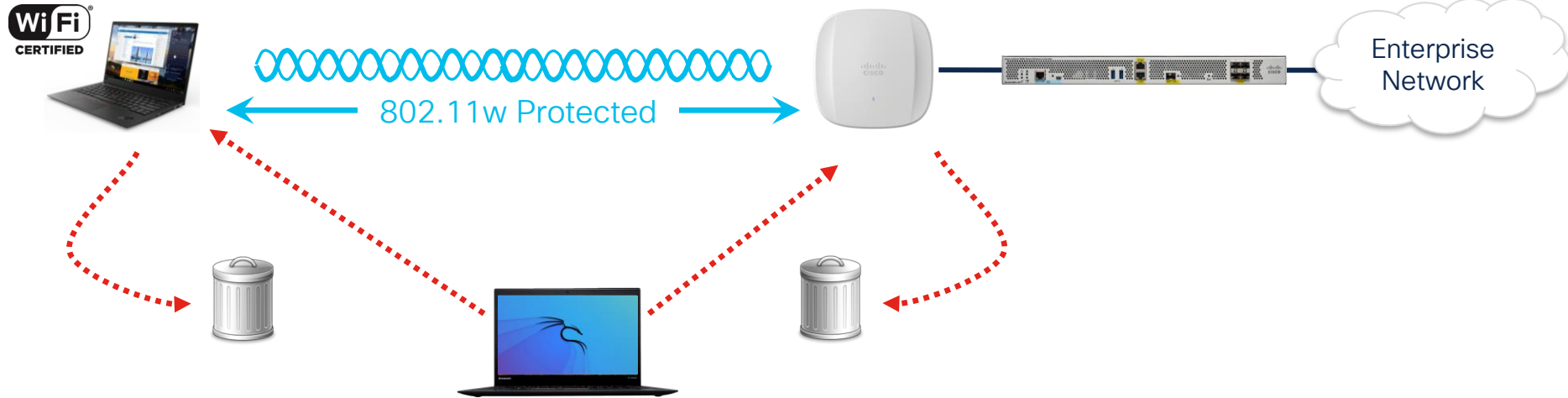
# Key Reinstallation Attack



- [10 Vulnerabilities were discovered](#)
  - May allow the reinstallation of keys already in use
- Only 1 impacts Access Points
  - Specific to 802.11r (Fast BSS Transition)
  - [CVE-2017-13082](#)

- This was an industry wide issue
  - Not specific to any one vendor
- WPA3 certification includes KRACK exploit testing
- The attacker positions a rogue AP clone to perform a MitM attack
  - This flaw causes all WPA2 encryption protocols to reuse the keystream when encrypting packets
- Rogue AP detection and WIDS/WIPS can detect potential attack vectors

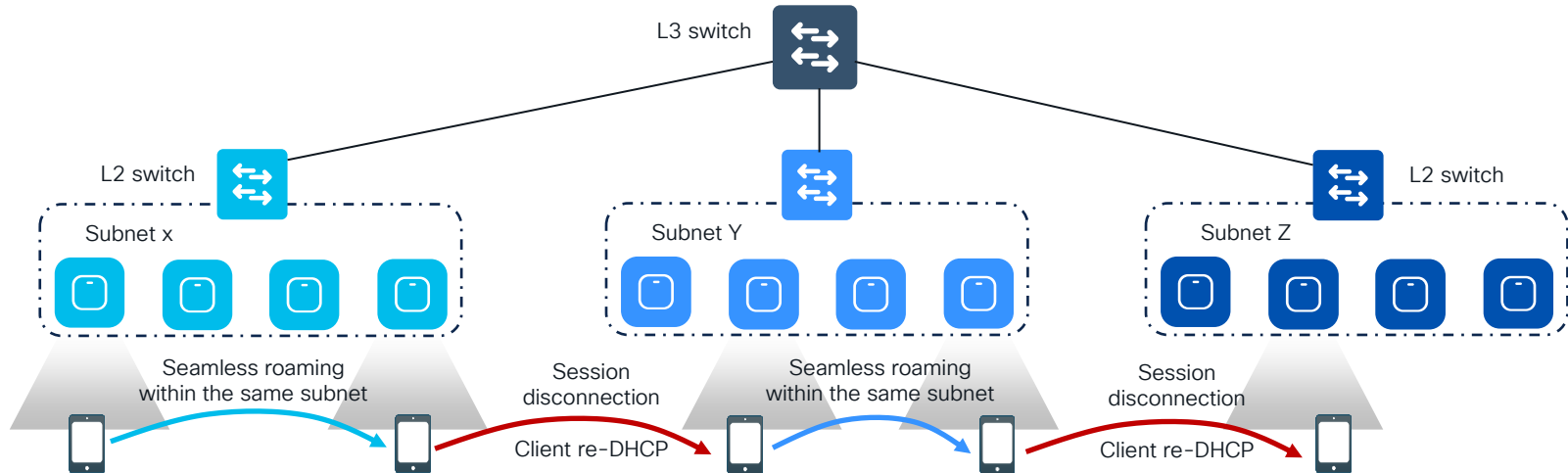
# 802.11w Protected Management Frames



# Seamless Roaming at Scale

For L2 seamless roaming everywhere need to span the same VLAN across all roaming domain

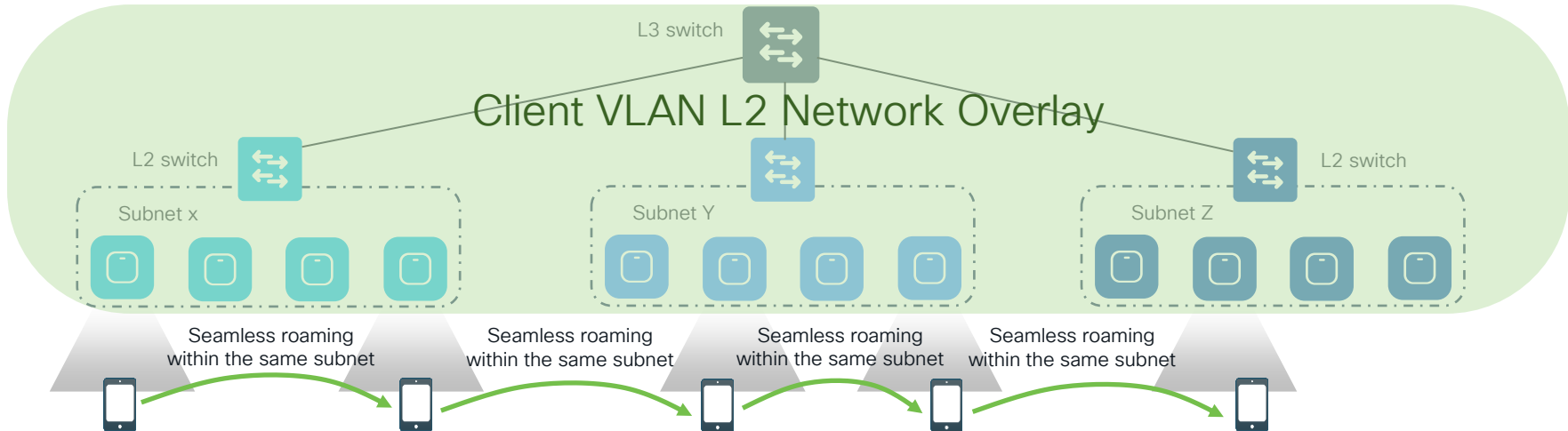
Large broadcast domains do not scale and is counter to networking best practice



# Seamless Roaming at Scale

For L3 seamless roaming an extended VLAN network overlay is required

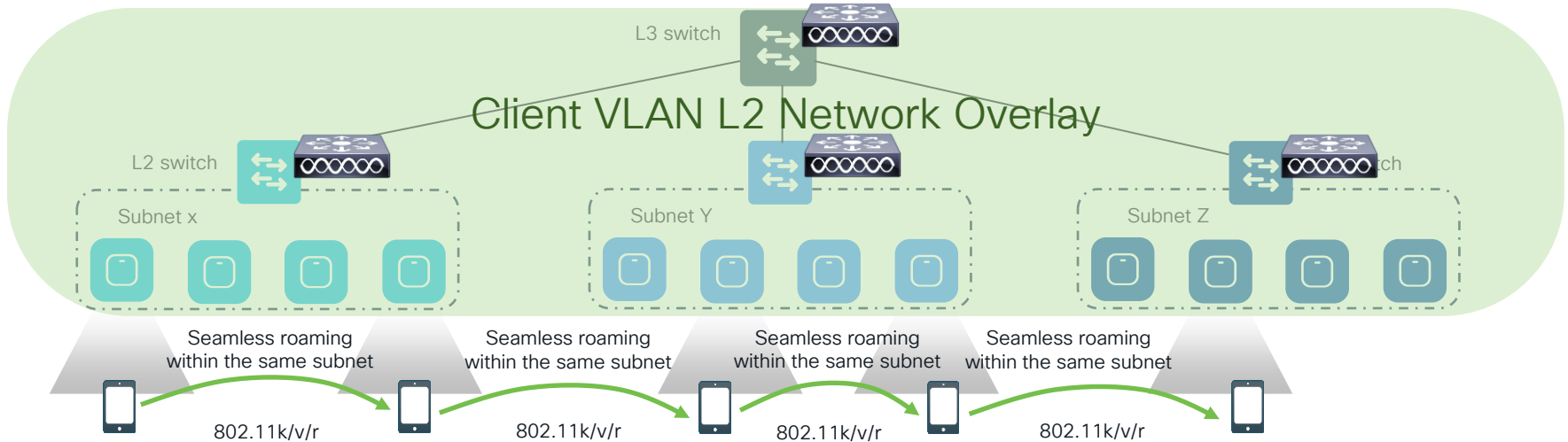
A data termination point is required to roam across L3 boundaries



# Seamless Roaming at Scale

Edge Wireless Service  
Data Plane (DP) Termination

Can be deployed as centralised  
(CAPWAP / EoGRE) or distributed  
(fabric) architectures



# On-Prem and Cloud Identity



## On-Prem Identity



802.1x, Network Access



PEAP-MSCHAPv2,  
EAP-FAST, EAP-TLS  
PAP, MAC Auth Bypass



## Cloud Identity

VPN, Application Access

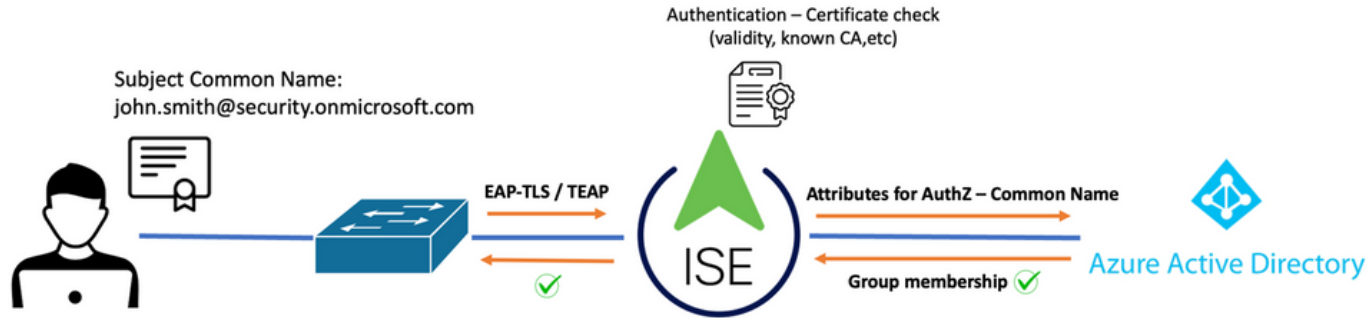


SAMLv2, OpenID Connect





# Cloud Identity with EAP-TLS



# Multi-Factor Authentication



# Zero Trust

41% of all data breaches resulted from cyber security incidents  
(162 notifications)

Cyber incident breakdown



- Ransomware

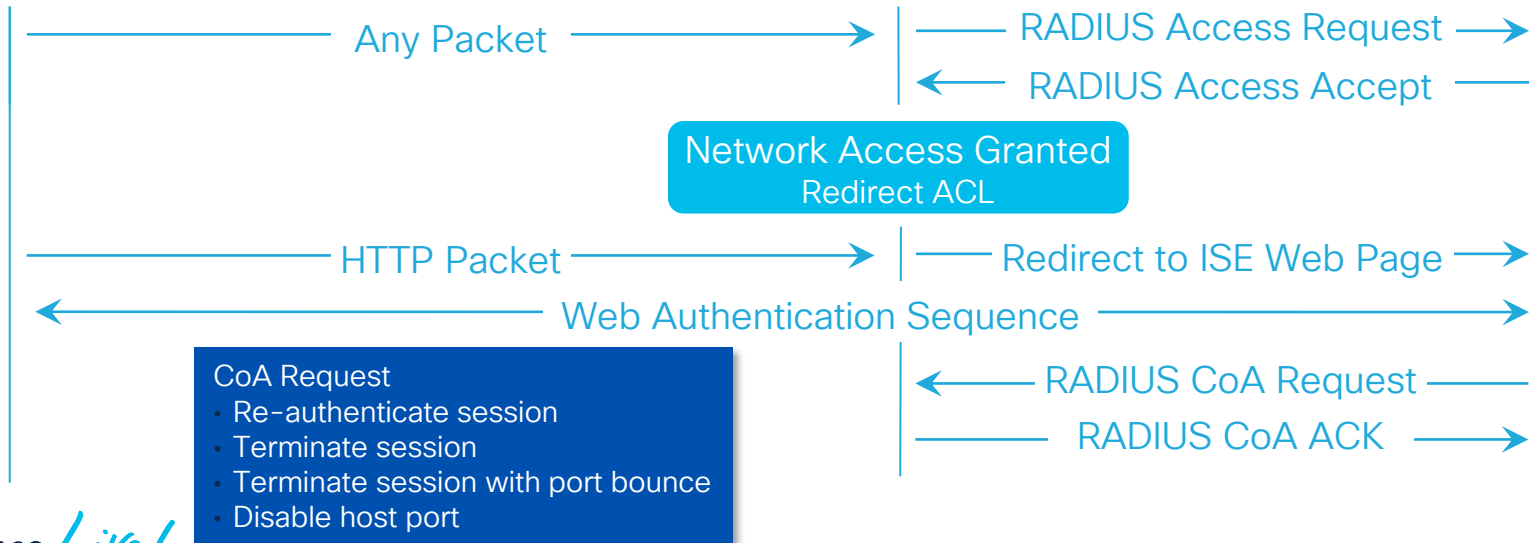
- East/West Traversal
- Authorisation
  - Micro-segmentation
- Rapid Threat Containment

CISCO *Live!*

- Phishing and compromised or stolen credentials
  - Username/Password
  - Digital Certificates

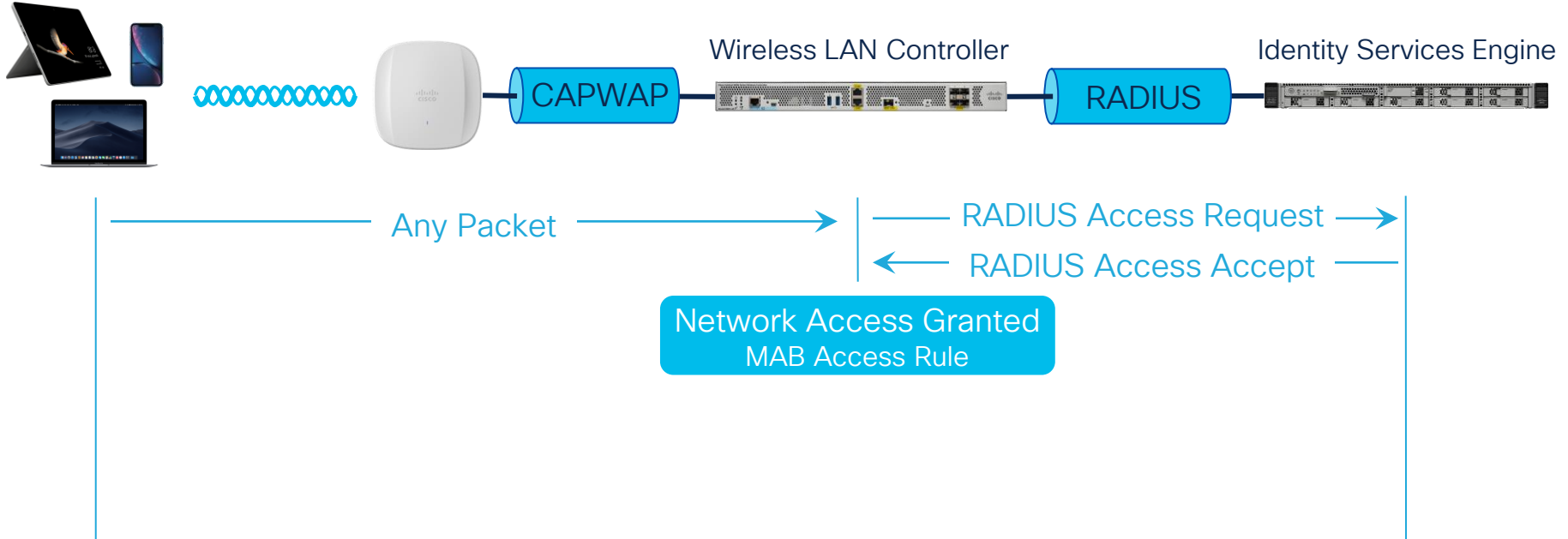
# Central Web Authentication

## URL Redirect



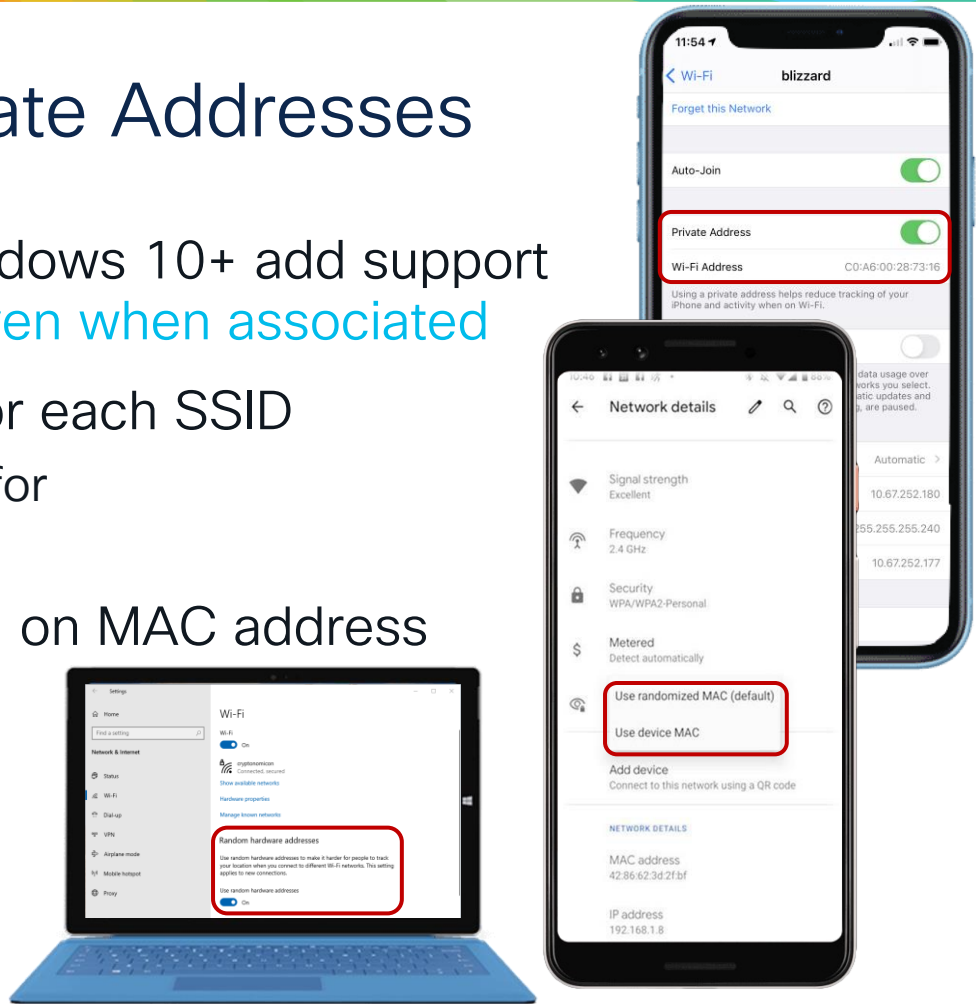
# Central Web Authentication

## MAC Authentication Bypass



# Random MAC and Private Addresses

- iOS 14+, Android 10+ and Windows 10+ add support for random MAC Addresses **even when associated**
- A random MAC is generated for each SSID
  - That MAC **may** remain constant for the saved profile
- This will impact services based on MAC address
  - MAC authentication bypass
  - Web authentication
  - Location analytics



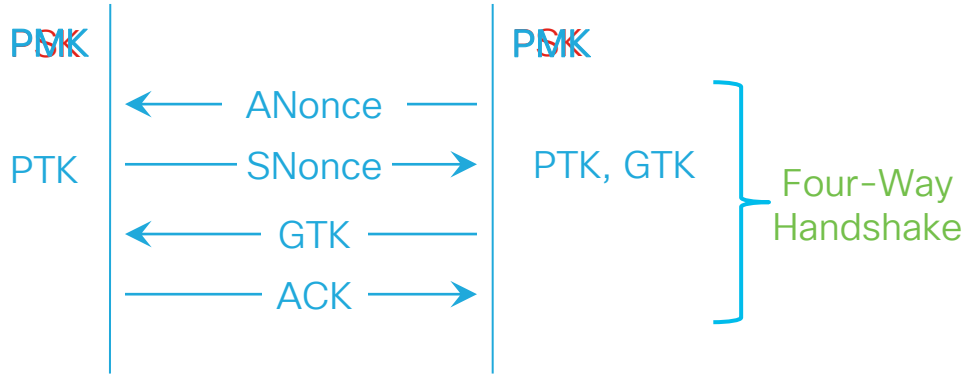
# WPA Personal

## Pre-Shared Key



# WPA Personal

## Pre-Shared Key

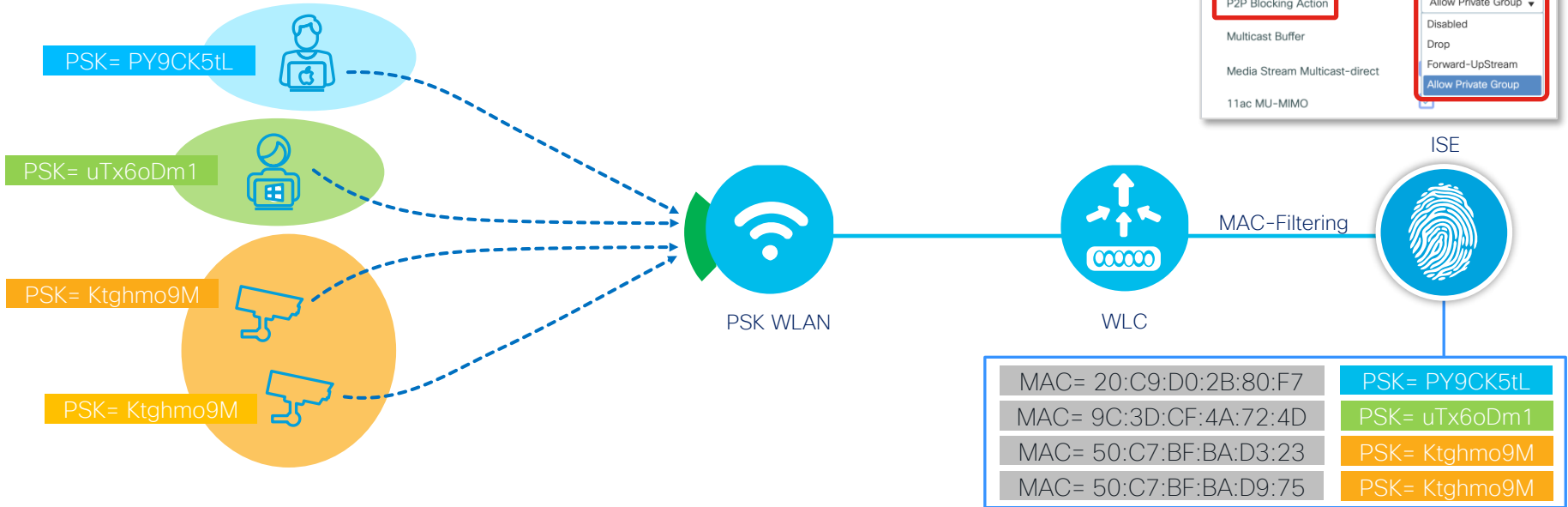


$$PTK = \text{SHA}(\text{PMK} + \text{ANonce} + \text{SNonce} + \text{AP MAC} + \text{STA MAC})$$

- Offline Attacks
  - Dictionary
  - Rainbow Table
- Strong Passwords Matter

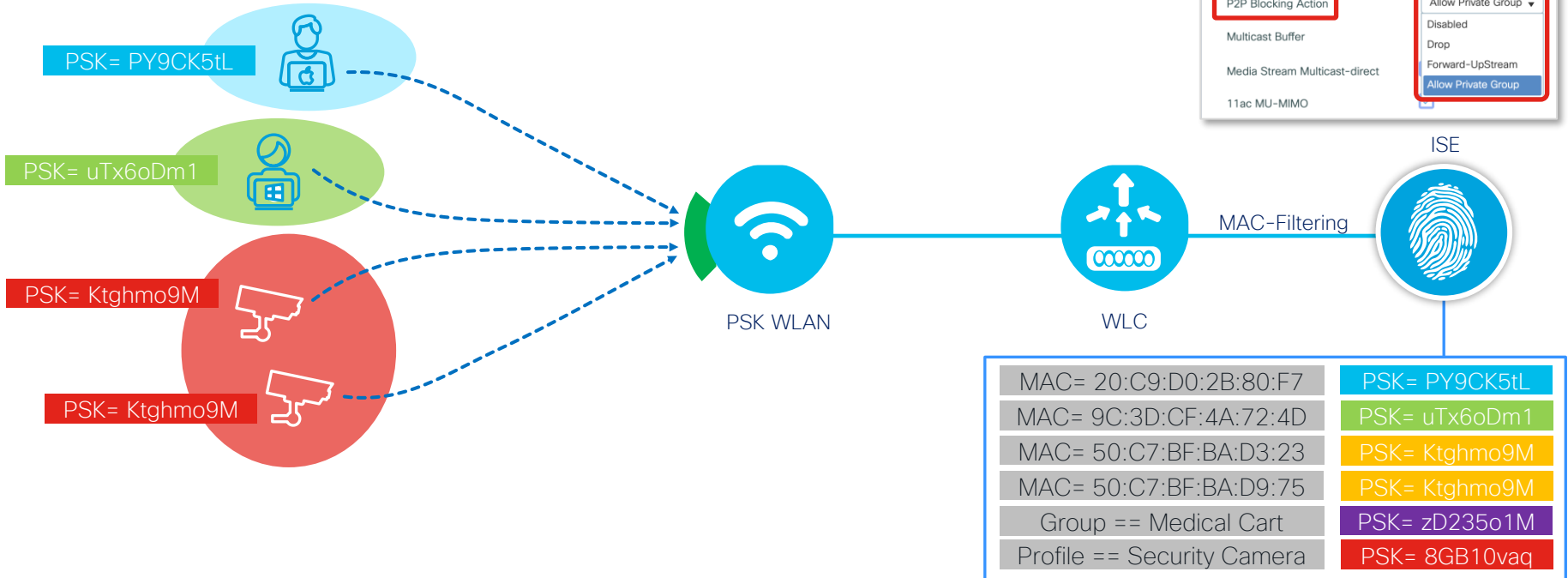


# Identity PSK



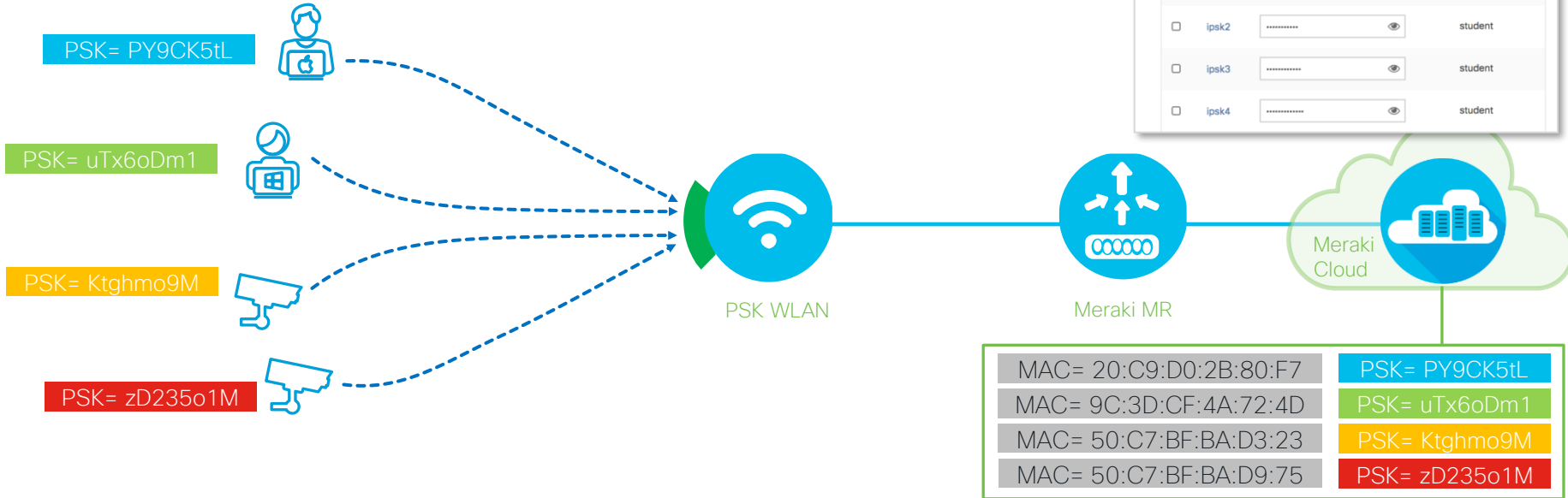
<https://www.cisco.com/c/en/us/support/docs/wireless/catalyst-9800-series-wireless-controllers/216130-configure-catalyst-9800-wlc-ipsk-with-ci.html>  
[https://documentation.meraki.com/MR/Encryption\\_and\\_Authentication/IPSK\\_with\\_RADIUS\\_Authentication](https://documentation.meraki.com/MR/Encryption_and_Authentication/IPSK_with_RADIUS_Authentication)

# Identity PSK



<https://www.cisco.com/c/en/us/support/docs/wireless/catalyst-9800-series-wireless-controllers/216130-configure-catalyst-9800-wlc-ipsk-with-ci.html>  
[https://documentation.meraki.com/MR/Encryption\\_and\\_Authentication/IPSK\\_with\\_RADIUS\\_Authentication](https://documentation.meraki.com/MR/Encryption_and_Authentication/IPSK_with_RADIUS_Authentication)

# Identity PSK without RADIUS



# Simultaneous Authentication of Equals

## WPA3

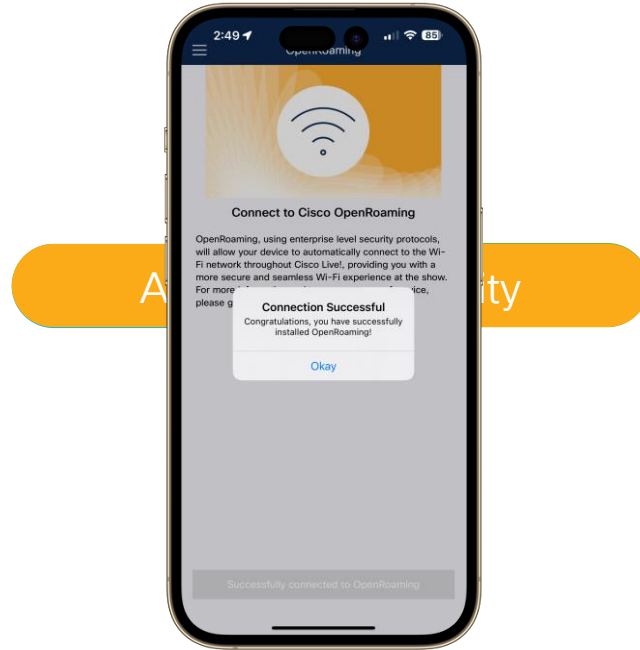
- Based on the Dragonfly Key Exchange
  - Balanced Password Authenticated Key Exchange
    - Security of SAE not tied to the complexity of the shared secret
  - SAE exchanges results in a 32-byte PMK
    - Protects against offline dictionary attacks
    - Forward secrecy protects traffic if the password is compromised in future
    - Supports Protected Management Frames
- WPA3-SAE Transition Mode supports both WPA2-PSK and WPA3-SAE on the same SSID
  - Transition Disable will prevent WPA3-Personal clients from downgrading to WPA2-Personal on roams mitigating downgrade attacks

# Wi-Fi Certified Enhanced Open

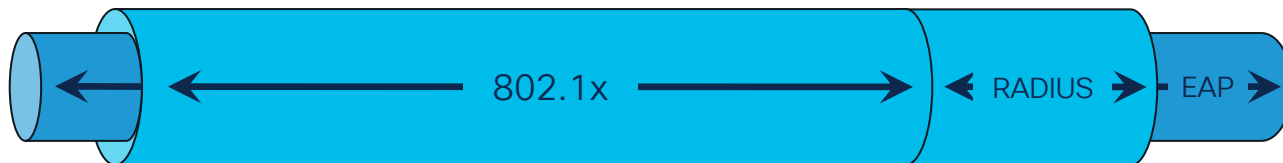
## WPA3

- Opportunistic Wireless Encryption (OWE)
  - Replaces 802.11 “open” authentication support
  - Client and AP perform an unauthenticated Diffie-Hellman Key Exchange to establish a PMK
  - Four-Way Handshake used as normal
  - Supports Protected Management Frames
- Diffie-Hellman is susceptible to MitM attacks
  - Would allow the attacker same visibility as on an Open network

# Decoupling Access and Identity



# OpenRoaming



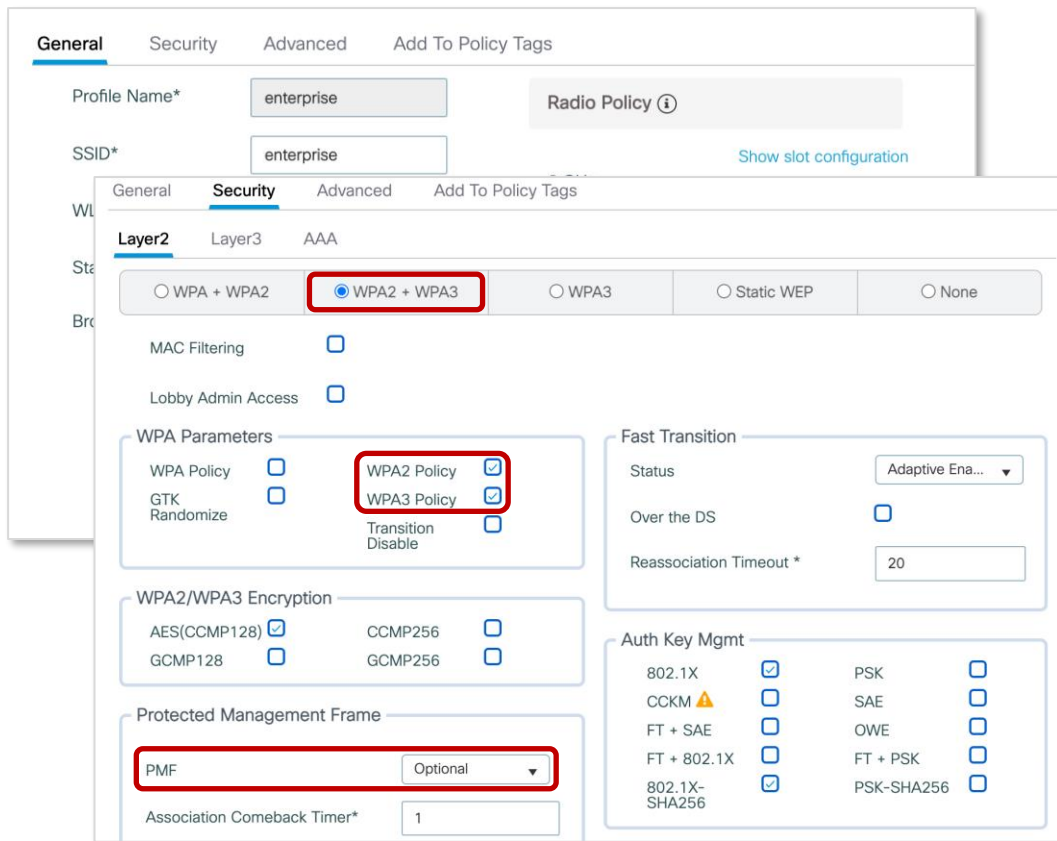
# Implications of 6GHz



WPA3 and OWE are **mandatory** for 6GHz



WPA2 and Open are **not** supported on 6GHz

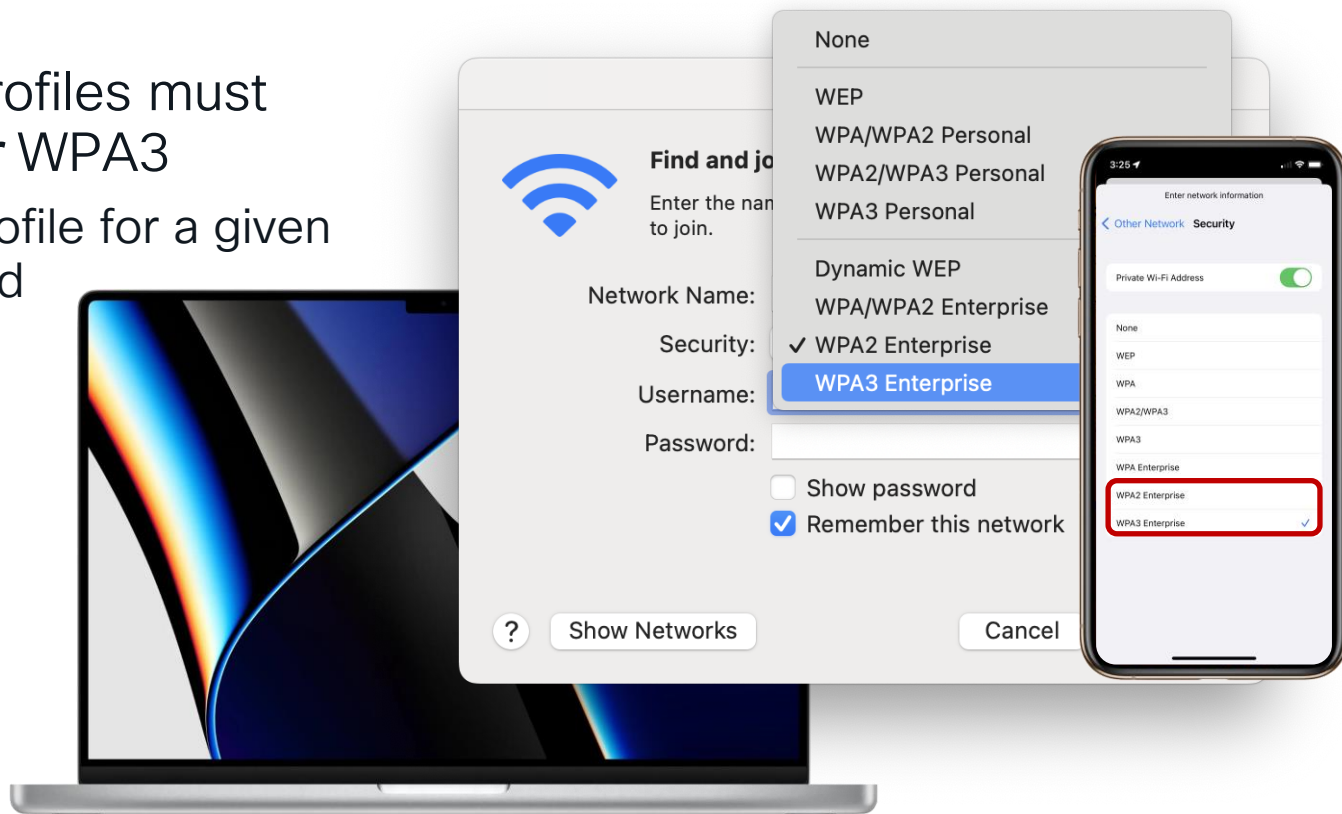


The screenshot displays the Cisco Wi-Fi configuration interface, specifically the Security tab. The configuration is for a profile named 'enterprise'. The Security tab is selected, and the Layer2 sub-tab is active. The security mode is set to 'WPA2 + WPA3', which is highlighted with a red box. Under WPA Parameters, both 'WPA2 Policy' and 'WPA3 Policy' are checked, also highlighted with a red box. The WPA2/WPA3 Encryption section shows 'AES(CCMP128)' and 'GCMP128' as options. The Protected Management Frame (PMF) is set to 'PMF' with a dropdown menu, highlighted with a red box. The Association Comeback Timer is set to 1. The Fast Transition section shows 'Adaptive Enable' as the status. The Auth Key Mgmt section shows '802.1X' and 'PSK' as options.



# Wi-Fi 6E and Wi-Fi 7 Security

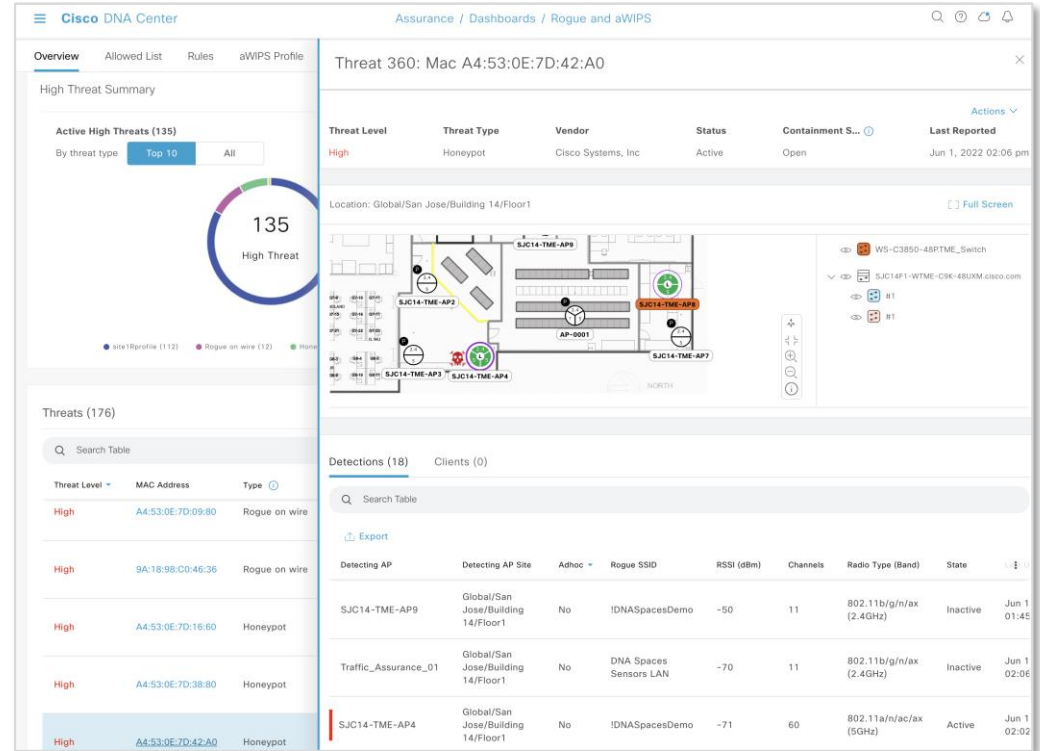
- Client device profiles must select WPA2 *or* WPA3
- And only one profile for a given SSID is permitted



# Rogue Detection and Advanced WIPS

# Rogue Detection and Advanced WIPS

- Centralized wireless threat management
- Rogue detection and classification
- Rogue location and mitigation
- Monitor and classify threats
- Event correlation
- Security compliance reporting



[https://www.cisco.com/c/en/us/td/docs/cloud-systems-management/network-automation-and-management/dna-center-rogue-management-application/2-3-3/quick-start-guide/b\\_rogue\\_management\\_qsg\\_2\\_3\\_3.html](https://www.cisco.com/c/en/us/td/docs/cloud-systems-management/network-automation-and-management/dna-center-rogue-management-application/2-3-3/quick-start-guide/b_rogue_management_qsg_2_3_3.html)

# Rogue Detection and Advanced WIPS

- Wireless threat detection
- Forensic capture
- Client exclusion policies

Configuration > Security > Wireless Protection Policies

Rogue Policies Rogue AP Rules Client Exclusion Policies

Select all events ☒

Excessive 802.11 Association Failures ☒

Excessive 802.1X Authentication Failures ☒

Excessive 802.1X Authentication Timeout ☒

IP Theft or IP Reuse ☒

Excessive Web Authentication Failures ☒

Captures (11)

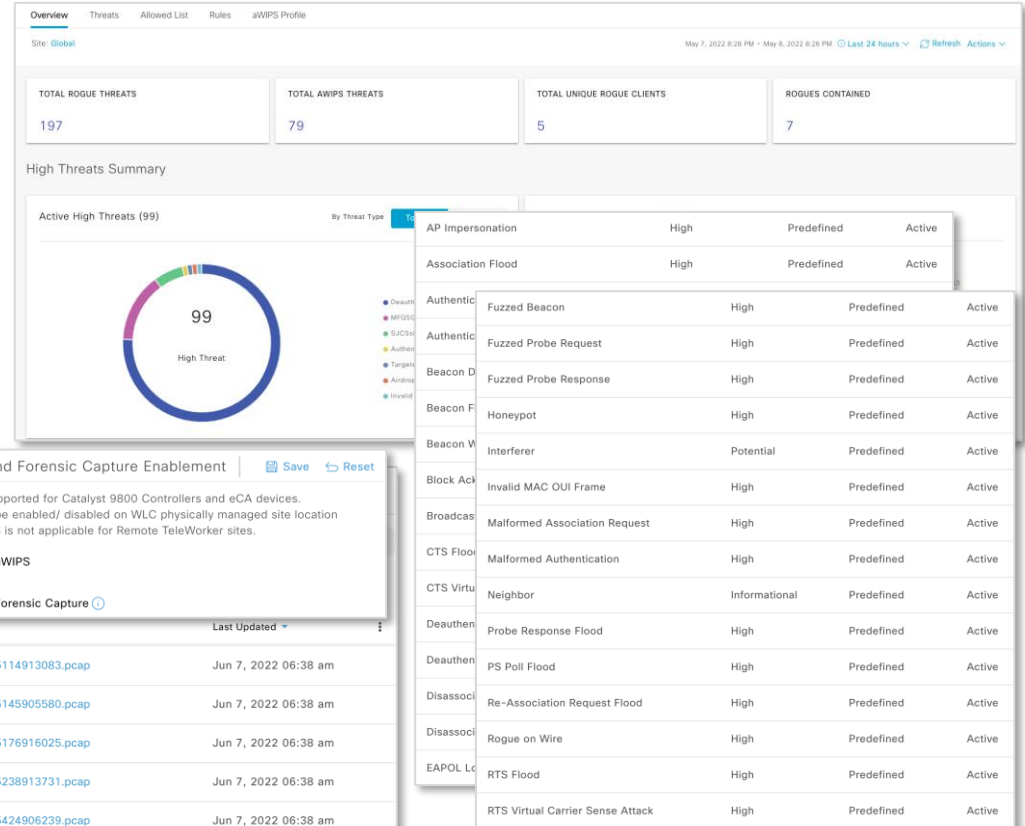
Alarm ID	Capture Filename	Last Updated
226034	A0F8497EC066_80211_1622535114913083.pcap	Jun 7, 2022 06:38 am
226035	A0F8497EC066_80211_1622535145905580.pcap	Jun 7, 2022 06:38 am
226036	A0F8497EC066_80211_1622535176916025.pcap	Jun 7, 2022 06:38 am
PLS06-AP3800-01	A0F8497EC066_80211_1622535238913731.pcap	Jun 7, 2022 06:38 am
PLS06-AP3800-01	A0F8497EC066_80211_1622535424906239.pcap	Jun 7, 2022 06:38 am

aWIPS and Forensic Capture Enablement

aWIPS is supported for Catalyst 9800 Controllers and eCA devices.  
aWIPS can be enabled/ disabled on WLC physically managed site location  
Note: aWIPS is not applicable for Remote TeleWorker sites.

☒ Enable aWIPS

☒ Enable Forensic Capture



# Rogue Access Points

- A **Rogue AP** is any AP which is not part of our infrastructure
  - Most of them will be legitimate
  - Some of them may be malicious
- Correctly differentiating between the two is critical

The screenshot displays the 'Add AP Join Profile' configuration window, specifically the 'Security' tab. The 'Rogues' section is active, showing 'Rogue Detection' enabled with a checkbox. Below it, 'Rogue Detection Minimum RSSI' is set to -90 and 'Rogue Detection Transient Interval (seconds)' is set to 0. A second window, 'Wireless Protection Policies', is overlaid on top. In this window, the 'Rogue Policies' tab is selected, and 'Rogue AP Rules' is highlighted with a red box. The 'General' sub-tab is active, showing various detection settings like 'Rogue Detection Security Level' (Custom), 'Expiration timeout for Rogue APs (seconds)\*' (1200), and 'Rogue Polling Interval (seconds)' (3600). The 'Auto Contain' sub-tab is also visible, showing 'Auto Containment Level' (1) and 'Auto Containment only for Monitor Mode APs' (unchecked). A red box highlights the 'Using our SSID' checkbox under 'Auto Containment only for Monitor Mode APs'. The 'MFP Configuration' section at the bottom shows 'Global MFP State' (unchecked), 'AP Impersonation Detection' (unchecked), and 'MFP Key Refresh Interval (hours)\*' (24).

# Rogue Clients

- A **Rogue Client** is any client which is connected to a Rogue AP
- What we care about are **our** clients which have connected to the Rogue AP
- But this is not necessarily a risk

- Clients may create ad-hoc wireless networks
- This can be a risk if they have bridged to the wired network

Configuration > Security > Wireless Protection Policies

**Rogue Policies**   Rogue AP Rules   Client Exclusion Policies

**General**

Rogue Detection Security Level	Custom
Expiration timeout for Rogue APs (seconds)*	1200
Validate Rogue Clients against AAA	<input checked="" type="checkbox"/>
Validate Rogue APs against AAA	<input checked="" type="checkbox"/>
Rogue Polling Interval (seconds)	3600
Detect and Report Adhoc Networks	<input checked="" type="checkbox"/>
Rogue Detection Client Number Threshold*	0
Rogue Init Timer (seconds)*	180
AP Authentication	<input checked="" type="checkbox"/>
AP Authentication Alarm Threshold*	1
Syslog Notification	<input checked="" type="checkbox"/>

**Auto Contain**

Auto Containment Level	1
Auto Containment only for Monitor Mode APs	<input type="checkbox"/>
Using our SSID	<input checked="" type="checkbox"/>
Valid client on Rogue AP	<input checked="" type="checkbox"/>
Adhoc Rogue AP	<input checked="" type="checkbox"/>

**MFP Configuration**

Global MFP State	<input type="checkbox"/>
AP Impersonation Detection	<input type="checkbox"/>
MFP Key Refresh Interval (hours)*	24

Apply

# Cisco Catalyst Centre Threat Levels

## Informational

- RSSI  $\leq -75$  dBm and not on wire
- Rogue Type: Neighbor

## Potential

- RSSI  $> -75$  dBm and not on wire
- Rogue Type: Interferer

## High

- Rogue Types
  - Honeypot
  - Impersonation AP
  - Rogue on wire
  - Beacon DS attack
- All WIPS threats

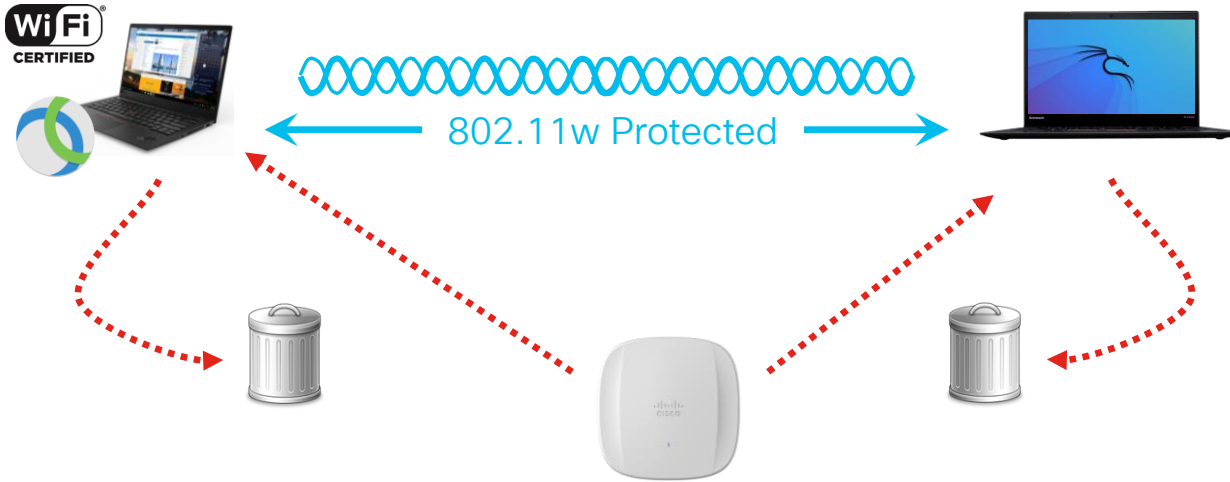
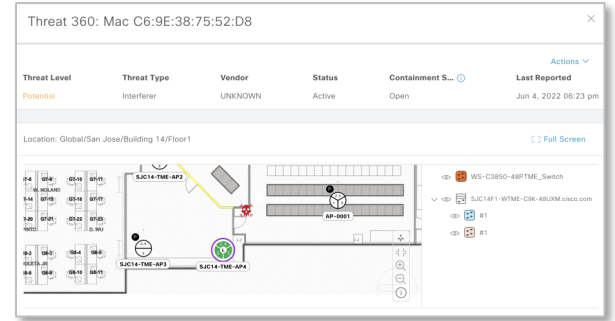
# Rogue AP Containment

- How do we contain Rogue APs?
  - Containment is a spoofed 802.11 disassociation/deauthentication request attack
- How does WPA3 affect Rogue AP containment?
  - 802.11w will change how we can mitigate Rogue AP related threats
  - The ability to physically locate rogues will be key

The screenshot displays the Cisco DNA Center interface, specifically the 'Assurance / Dashboards / Rogue and aWIPS' section. The main view shows a table of threats, with 'Threat 360: Mac A4:53:0E:7C:99:E0' selected. A warning dialog box is overlaid, stating: 'Warning: Using this feature may have legal consequences. Wireless containment will be initiated for the below rogue BSSIDs on wireless controller with IP address 172.20.224.55. Do you want to'. Below the warning, another threat entry is visible: 'Threat 360: Mac C6:9E:38:75:52:D8' with a 'Potential' threat level and 'Interferer' threat type. The interface also shows a floor plan of 'Global/San Jose/Bldg 14/Floor1' with various access points (AP-0001, SJC14-TME-AP2, SJC14-TME-AP3, SJC14-TME-AP4) and switches (WS-C3850-48PTME\_Switch, SJC14F1-WTME-C9K-48UXM) marked. A red circle highlights a specific location on the floor plan.



# Rogue Containment with WPA3



# Rogue on Wire

- Matching Algorithms
  - MAC Address  $\pm 3/\pm 2/\pm 1$
  - Vendor matching algorithms
- Rogue AP in Bridge Mode
  - Locate the Rogue AP via the Rogue Client MAC address and Gateway MAC Address
- Wired 802.1x matters

The screenshot displays the Cisco DNA Center Assurance dashboard for 'Rogue and aWIPS'. The main view shows a 'Threat 360: Mac 6A:3A:0E:53:A6:E9' with a 'High' threat level. A table lists threat details:

Threat Level	Threat Type	Vendor	Status	Containment S...
High	Rogue on wire	UNKNOWN	Active	Open

Below the table, a floor plan visualization shows the location of the threat at 'Global/San Jose/Building 14/Floor1'. A red box highlights the 'Shutdown Switchport' action in the 'Actions' menu.

The 'Threats (134)' section shows a table of active threats:

Threat Level	MAC Address	Type
High	68:3A:1E:53:A6:E0	Rogue on wire
High	6A:3A:0E:53:A6:E9	Rogue on wire
High	9A:18:98:C0:46:36	Rogue on wire
High	A4:53:0E:7D:09:80	Rogue on wire

The 'Switch Port Detail (1)' section shows a table of switch port details:

Host Mac	Device Name	Device IP	Interface Name	Last Updated
70:F3:5A:7B:9F:71	WS-C3850-48PTME_Switch	172.20.224.156	GigabitEthernet5/0/47	Jun 5, 2022 09:40 am

# Air Marshal

- Rogue AP Detection
  - Rogue Containment
  - Wired Rogue
- WIDS/WIPS
  - Spoofed Management Frames
  - Malicious Broadcasts / DoS
  - Packet Floods

**Air Marshal**

[Configure](#) [Rogue SSIDs 24](#) [Other SSIDs 595](#) [Spoofs 31](#) [Malicious broadcasts 0](#) [Packet floods 0](#)

**24 rogue SSIDs** seen for the last 2 hours

Edit Search...

<input type="checkbox"/>	SSID ▲	Broadcast MACs	Last seen	First seen	Containment	Rogue because
<input type="checkbox"/>	AXE BLE testing	6e:3a:0e:ff:f8:f5 (and 1 other)	4 seconds ago	1 year ago	partial	Recently seen on LAN
<input type="checkbox"/>	IT Test WiFi	e0:cb:bc:49:35:b1 (and 1 other)	50 seconds ago	1 month ago	contained	Recently seen on LAN
<input type="checkbox"/>	j-bond-2-owe	c6:14:92:6e:ae:b2 (and 2 others)	15 seconds ago	2 months ago	partial	Recently seen on LAN
<input type="checkbox"/>	j-bond-3-sae	ca:14:a2:6e:ae:b0 (and 1 other)	15 seconds ago	3 weeks ago	partial	Recently seen on LAN
<input type="checkbox"/>	j-bond-5-1x	c6:14:92:6e:ae:a5 (and 4 others)	6 seconds ago	3 weeks ago	partial	Recently seen on LAN
<input type="checkbox"/>	j-bond-8-owe-8	c6:14:92:6e:ae:b8 (and 2 others)	7 seconds ago	3 weeks ago	partial	Recently seen on LAN
<input type="checkbox"/>	j-p1-bond-2-owe	c6:14:92:6e:ae:a2 (and 4 others)	57 seconds ago	3 weeks ago	partial	Recently seen on LAN
<input type="checkbox"/>	j-p1-bond-3-sae	c6:14:92:6e:ae:a3 (and 4 others)	57 seconds ago	3 weeks ago	partial	Recently seen on LAN
<input type="checkbox"/>	j-p1-bond-4-sae	c6:14:92:6e:ae:b4 (and 5 others)	12 seconds ago	22 hours ago	partial	Recently seen on LAN
<input type="checkbox"/>	Meraki Setup	00:18:0a:36:d9:3e (and 98 others)	a moment ago	1 year ago	partial	Recently seen on LAN

10 results per page < 1 2 3 >

Close

Map data ©2023 Google Terms Report a map error

**SSID** IT Test WiFi [edit](#)

**Containment** contained

**Last seen** Wednesday 11/29/2023 8:25 pm  
50 seconds ago

**First seen** Wednesday 10/18/2023 7:18 am  
1 month ago

**Channels** 1, 149

**VLANs** 0

**Broadcast MACs** e0:cb:bc:49:35:b1 [edit](#)  
e2:cb:ac:49:35:b1 [edit](#)


**Wired MACs** e0:cb:bc:49:35:b1

**Encryption** Open

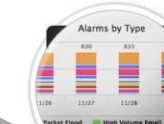
**Manufacturer** Cisco Meraki

**Rogue because** Recently seen on LAN

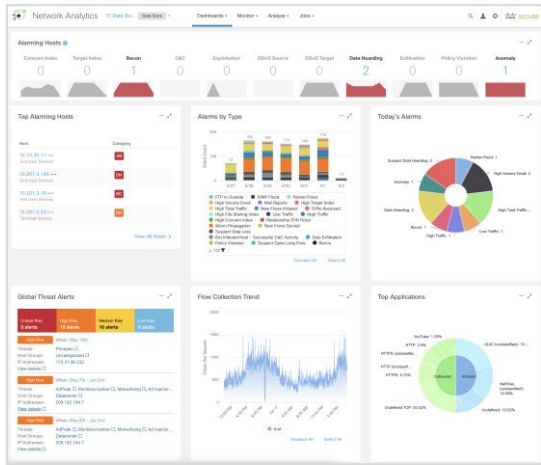
**Seen by** SFO12-1-AP08 (77 dB)  
SFO12-1-AP01 (41 dB)  
SFO12-1-AP03 (41 dB)  
SFO12-1-AP04 (41 dB)  
SFO12-1-AP05 (38 dB)  
SFO12-1-AP02 (34 dB)  
SFO12-1-AP07 (29 dB)  
SFO12-2-AP05 (12 dB)



Netflow



## Malware detection and cryptographic compliance on Cisco Stealthwatch



Top Security Events for 10.201.3.18							Source (5)	Target (1)
Security Event	Count	Concern Index	First Active	Target Host	Target Host Group	Actions		
Port Scan - 49155	50	540,000	06/02 3:51:05 PM	10.201.0.15 ***	Atlanta	...		
Port Scan - 53	16	172,800	06/02 3:51:05 PM	10.201.0.16 ***	Domain Controllers , Atlanta , DNS Servers	...		
Port Scan - 5355	2	21,600	06/02 4:48:48 PM	10.201.0.23 ***	Terminal Servers , Atlanta , Datacenter	...		
Ping	DNS Abuse							
Ping								
ICMP_Port_Unreach**	Alert Type Details							

1

DNS Abuse

Alert Type Details

Description

Device has been sending unusually large DNS packets. This alert uses the Unusual Packet Size observation and may indicate an attacker using the DNS protocol as a covert communications channel to exfiltrate data.

MITRE Tactics

Exfiltration

MITRE Techniques

Exfiltration Over Alternative Protocol

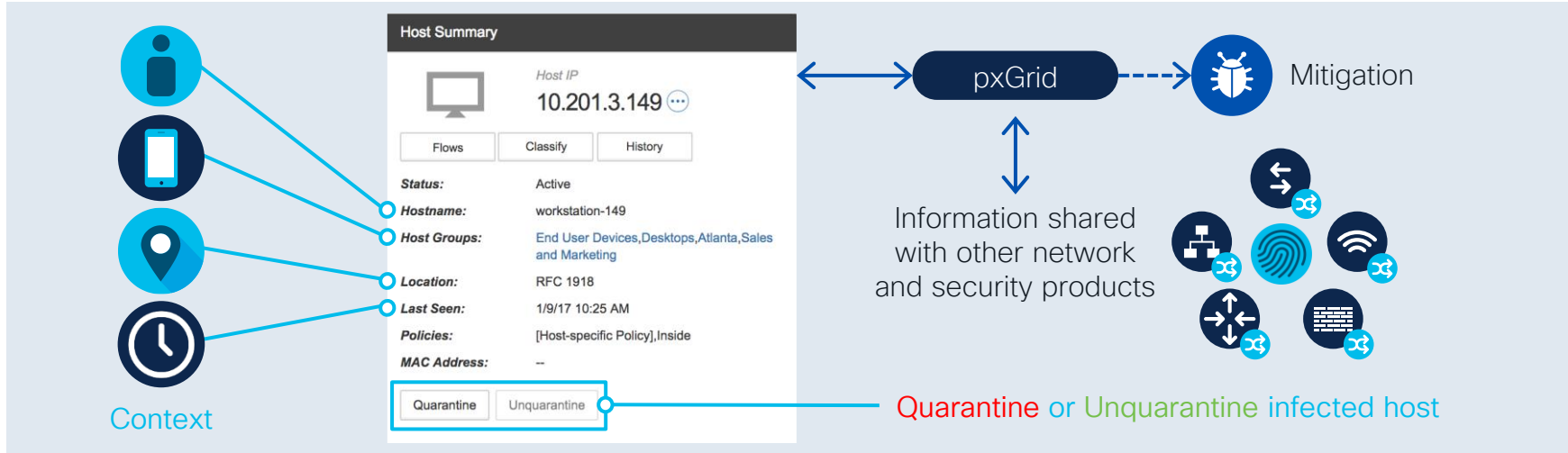
Alert Type Priority

Normal (Default)

go to alert priorities page

# Network as an Enforcer

## Rapid Threat Containment



Identity Services Engine



Secure Network Analytics Management Console

# Securing the Wireless Network



Secure the  
Air



Secure the  
Devices



Secure the  
Network





The bridge to possible

# Thank you

CISCO *Live!*

# Continue your education

**CISCO** *Live!*

## START

Monday, February 5 | 2:15 p.m.

### **TECEWN-3369**

TAC stories : WiFi networks that save lives...and your job

Tuesday, February 6 | 8:00 a.m.

### **BRKEWN-2014**

Meraki Wireless AIOps - An Intuitive AI Solution to Optimize Wi-Fi at Scale !

Tuesday, February 6 | 4:45 p.m.

### **BRKEWN-2029**

Cisco Wireless AIOps

Wednesday, February 7 | 4:00 p.m.

### **BRKEWN-2097**

Monitoring Catalyst Wireless with the Meraki Dashboard

Thursday, February 8 | 10:45 a.m.

### **BRKEWN-2667**

Cisco Wireless Supercharged by Cisco Catalyst Center - The Ultimate Guide to Bring Your Wireless Operation to the Next Level

Thursday, February 8 | 1:30 p.m.

### **BRKEWN-2043**

Saving Energy and Money with Your Cisco Wireless Network

Friday, February 9 | 9:00 a.m.

### **BRKEWN-3628**

Troubleshoot Catalyst 9800 Wireless Controllers

Friday, February 9 | 11:00 a.m.

### **BRKEWN-2399**

Meraki Wireless from a Troubleshooter Perspective

Friday, February 9 | 11:00 a.m.

### **BRKEWN-3006**

Keep your Catalyst 9800 & AP-COS Wireless Network Healthy, with Wireless Config Analyzer Express and other Advanced Tools

## FINISH



# Continue your education

CISCO *Live!*

## START

Monday, February 5 | 8:30 a.m.

### **TECEWN-2005**

Secure, Scalable, Enterprise Wi-Fi  
Deployment using Meraki Cloud

Tuesday, February 6 | 11:45 a.m.

### **IBOEWN-2031**

The Inner Workings of QoS for  
Modern Wireless Networks

Tuesday, February 6 | 1:15 p.m.

### **BRKEWN-2926**

Tune your Cisco Wi-Fi designs for  
the most demanding clients and  
applications, boosted with applied  
AI

Tuesday, February 6 | 2:00 p.m.

### **IBOEWN-2000**

Design/Deployment and tuning of  
Outdoor Wi-Fi & Workgroup  
Bridges (WGBs)

Tuesday, February 6 | 4:45 p.m.

### **BRKEWN-2035**

Meraki Wireless: Ready for  
Enterprise

Wednesday, February 7 | 2:15  
p.m.

### **BRKEWN-2042**

Cisco Spaces: How to Turn your  
Wi-Fi Network into Location Based  
Intelligence

Wednesday, February 7 | 2:15  
p.m.

### **IBOEWN-2349**

An Open Discussion on Shaping  
the Future of Buildings with Cisco  
Spaces

Thursday, February 8 | 8:30 a.m.

### **BRKEWN-3004**

Understanding Wireless Security  
and the Implications for Secure  
Wireless Network Design

Thursday, February 8 | 8:45 a.m.

### **BRKOPS-2402**

Automate the Deployment of a  
Wireless Network with the Help of  
Cisco Catalyst Center

Thursday, February 8 | 5:00 p.m.

### **BRKEWN-2037**

Open Roaming under the hood

## FINISH

The background features a vibrant, multi-colored abstract design. On the left, there are overlapping, wavy shapes in shades of red, orange, and yellow. On the right, a bright white light source emits a series of colorful rays in shades of blue, green, and yellow, creating a sunburst effect. The overall composition is dynamic and energetic.

cisco *Live!*

Let's go