

Understanding Wireless Security

and the Implications for Secure Wireless Network Design

cisco Live !

Mark Krischer
Principal Solutions Engineer

Cisco Webex App

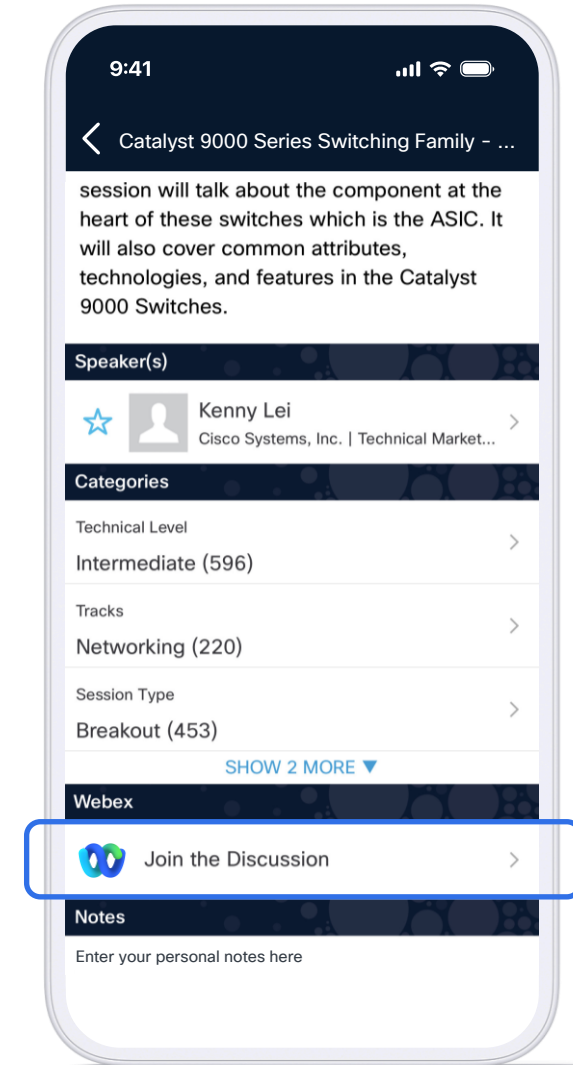
Questions?

Use Cisco Webex App to chat with the speaker after the session

How

- 1 Find this session in the Cisco Live Mobile App
- 2 Click “Join the Discussion”
- 3 Install the Webex App or go directly to the Webex space
- 4 Enter messages/questions in the Webex space

Webex spaces will be moderated by the speaker until 14 November 2025.



<https://ciscolive.ciscoevents.com/ciscolivebot/#BRKEWN-2104>

Agenda

- 1 Wireless Security Fundamentals**
 - WPA3
 - Authentication and Authorisation
 - Implications of 6GHz
- 2 Wireless Intrusion Detection and Prevention**
 - Rogue Detection and Mitigation
 - Advanced WIPS
 - Air Marshal
- 3 Network as a Sensor and Enforcer**

Wireless Security Fundamentals

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

Securing the Wireless Network



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 – Extensible Authentication Protocol)

WPA3

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

WPA3



- Mandatory for Wi-Fi 6 and Wi-Fi 7 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



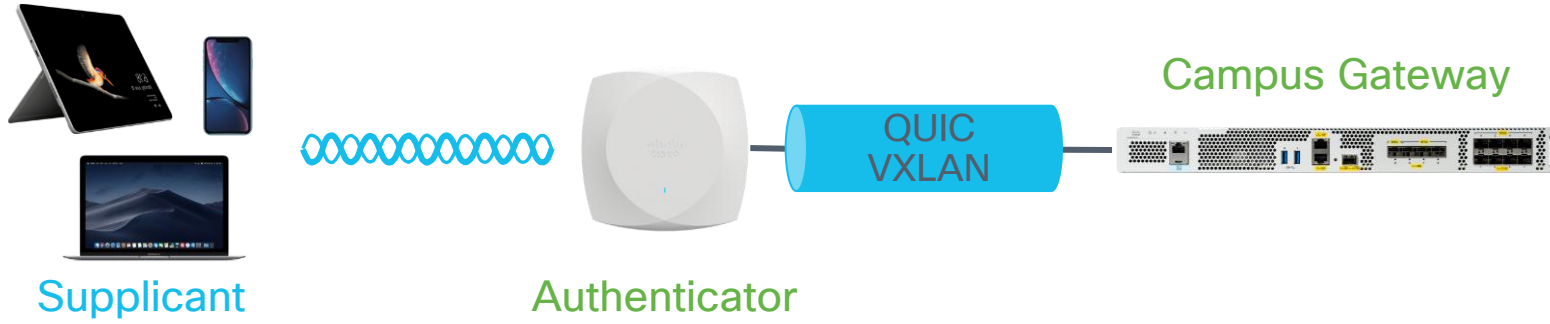
802.11 Fundamentals

Authentication



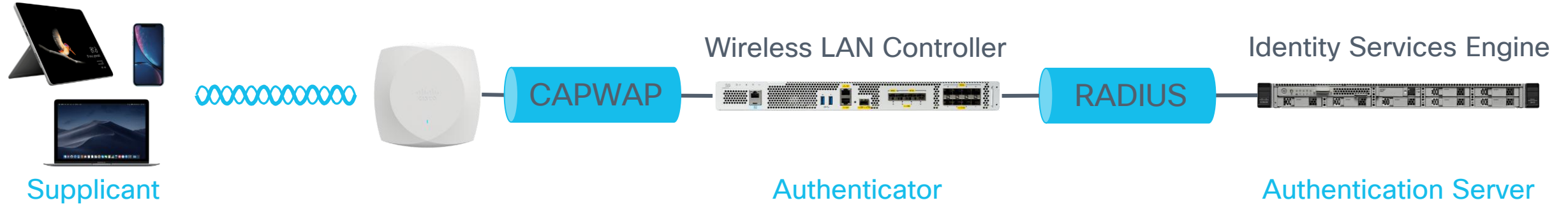
802.11 Fundamentals

Authentication



802.11 Fundamentals

Authentication



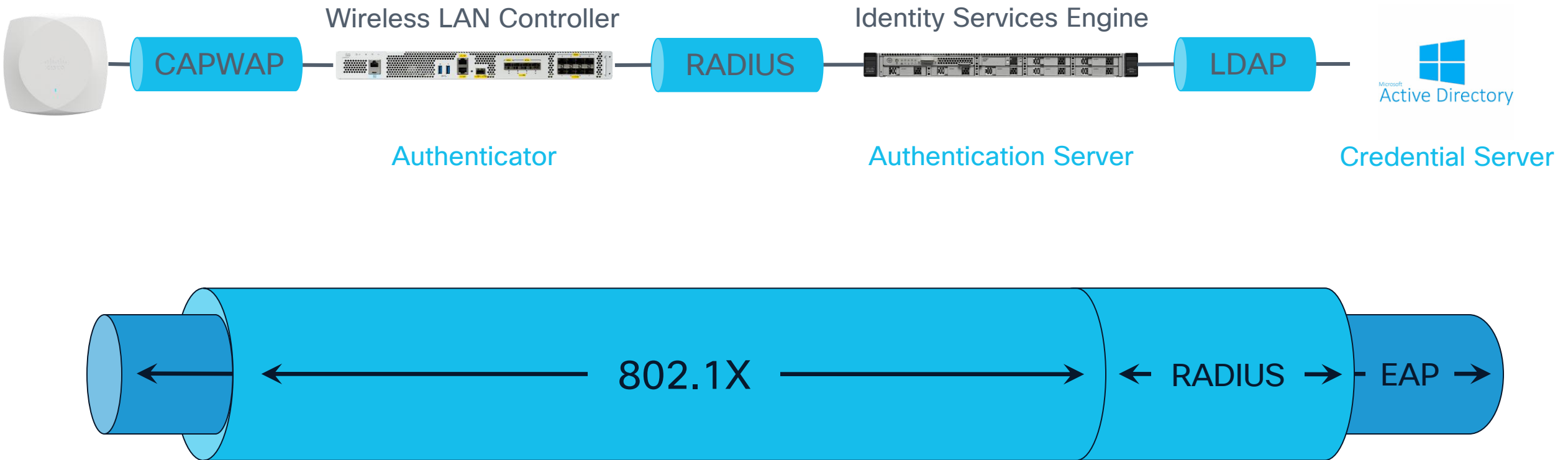
802.11 Fundamentals

Authentication



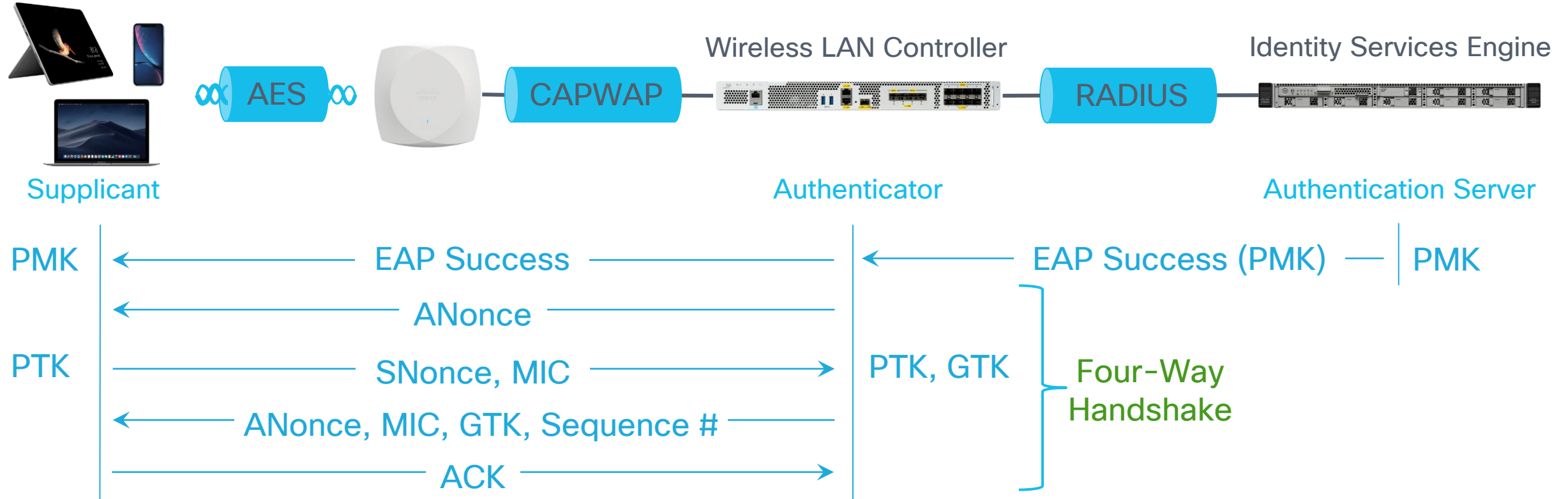
802.11 Fundamentals

Authentication



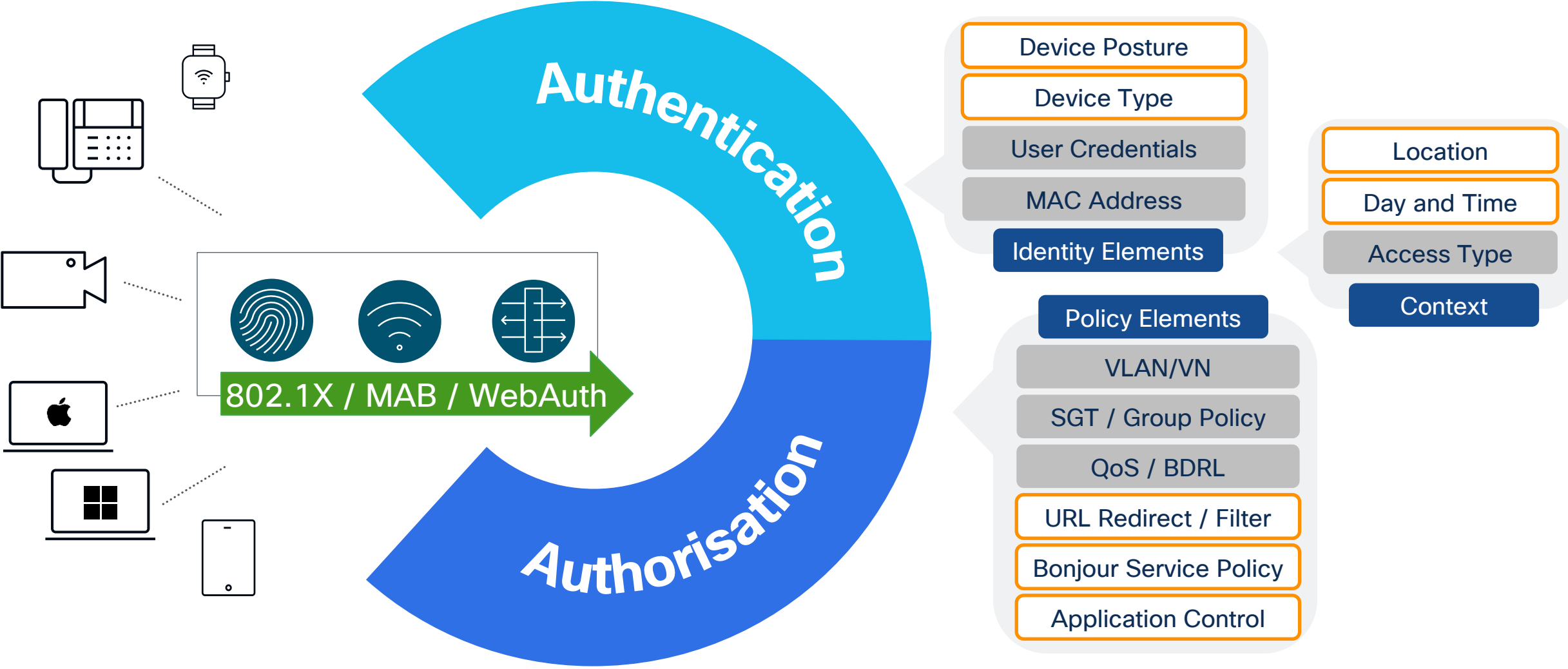
802.11 Fundamentals

Encryption



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

Authentication and Authorisation



Authorisation

Network Segmentation

Static VLAN Assignment

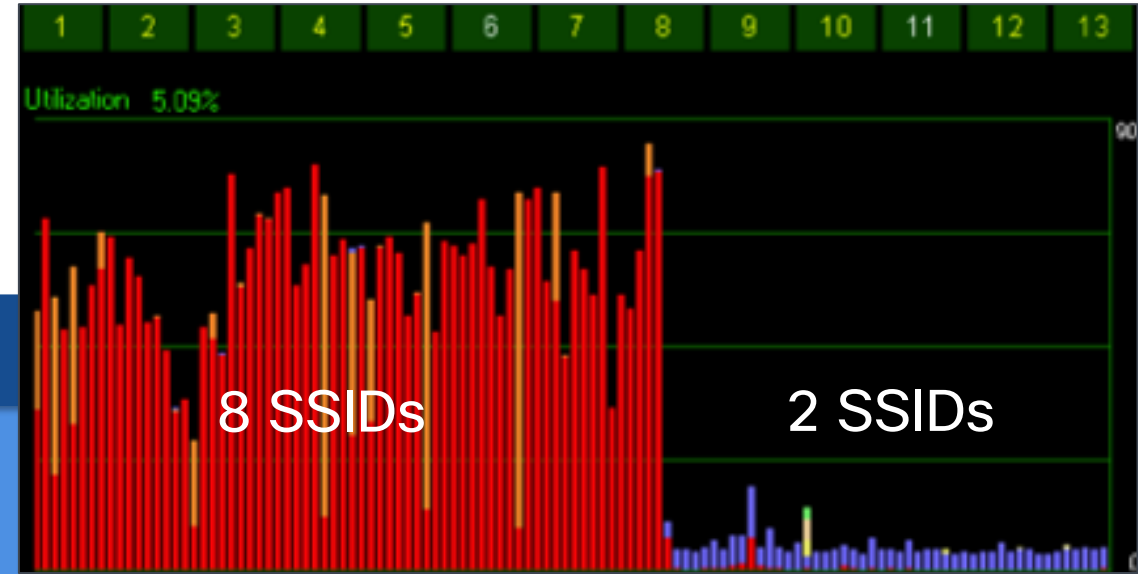
- VLAN based on SSID
- VLAN segregation based on security policy

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)



ISE Personas

Standalone ISE Node



Policy Administration Node (PAN)

- Single plane of glass for ISE admin
- Replication hub for all config changes



Monitoring & Troubleshooting Node (MnT)

- Reporting and logging node
- Syslog collector from ISE Nodes



Policy Services Node (PSN)

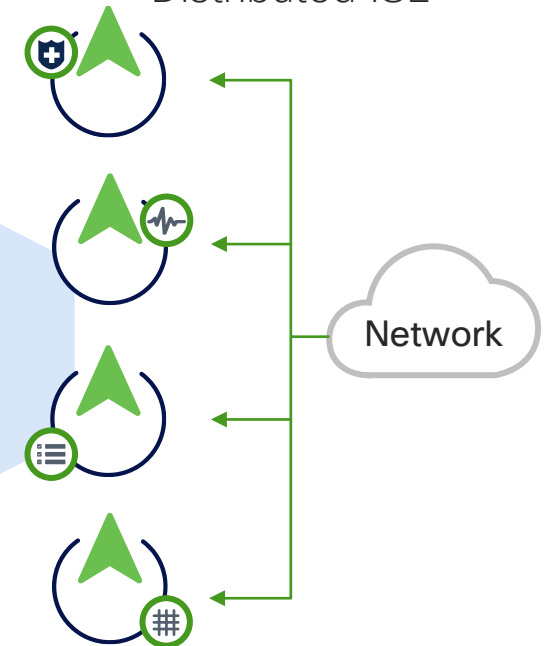
- Makes policy decisions
- RADIUS / TACACS+ Servers



pxGrid Controller (PXG)

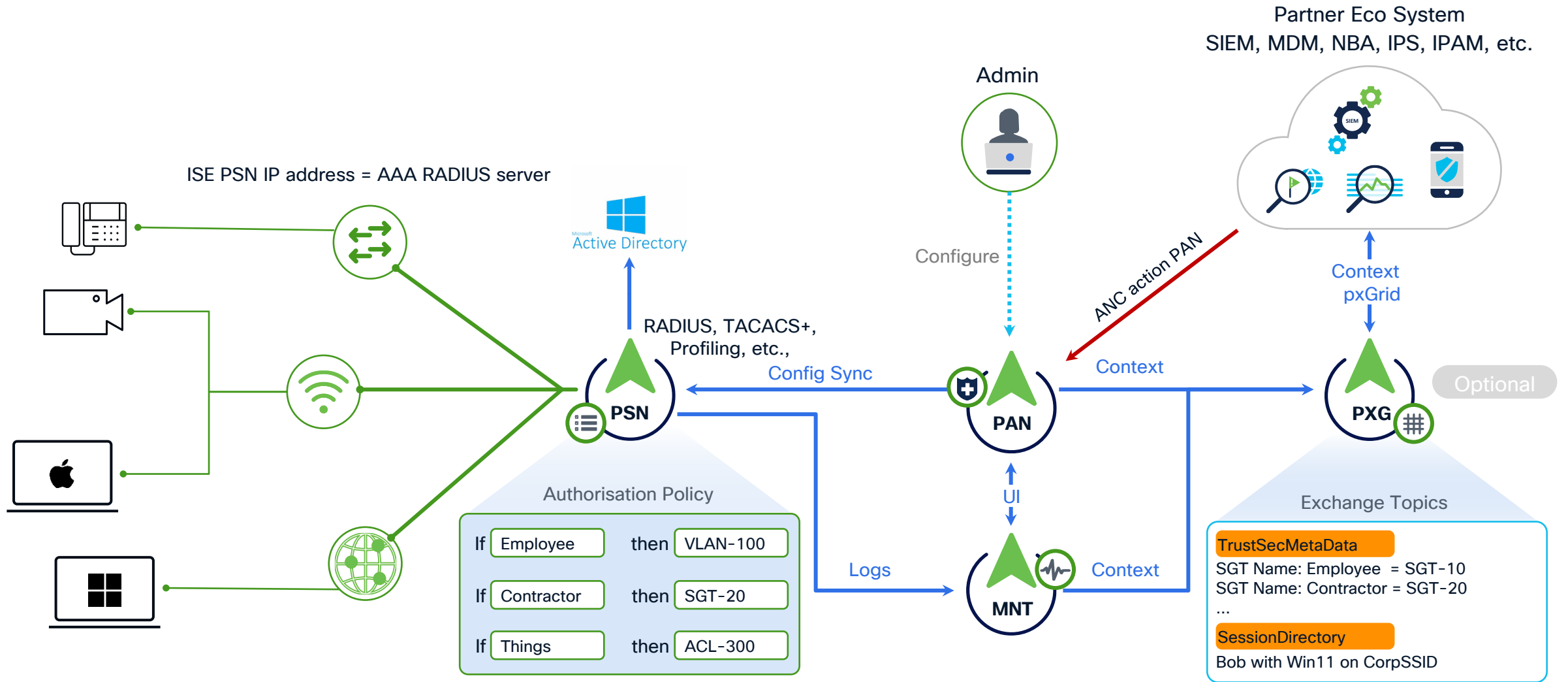
- Facilitates sharing of context

Distributed ISE

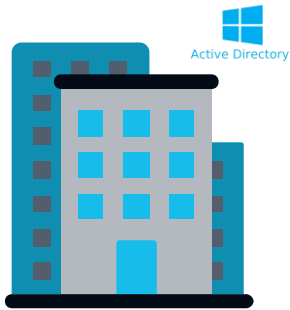


- Standalone provides no redundancy
 - Use for demo, testing, and lab purposes

ISE Architecture



On-Prem and Cloud Identity



On-Prem Identity



802.1X, Network Access



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



Cloud Identity

VPN, Application Access



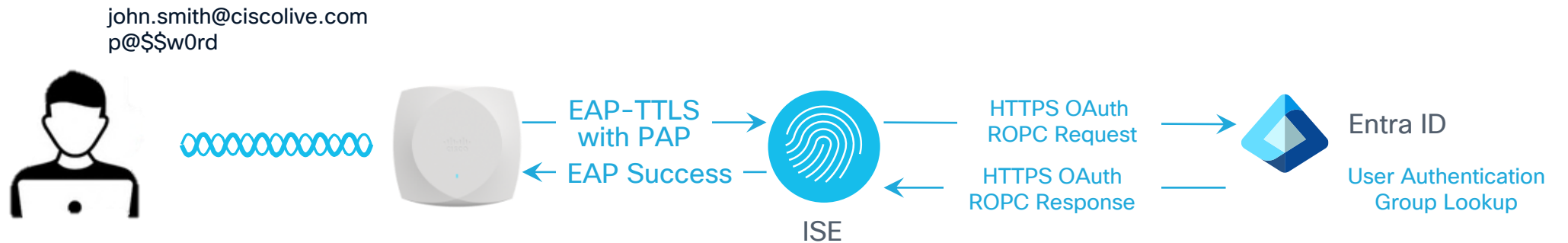
SAMLv2, OpenID Connect



Cloud Identity with EAP-TTLS

⚠ Warning

Microsoft recommends you do *not* use the ROPC flow. In most scenarios, more secure alternatives are available and recommended. This flow requires a very high degree of trust in the application, and carries risks that are not present in other flows. You should only use this flow when other more secure flows aren't viable.



<https://www.cisco.com/c/en/us/support/docs/security/identity-services-engine/216182-configure-ise-3-0-rest-id-with-azure-act.html>

MS-CHAPv2 Brute Force Attack

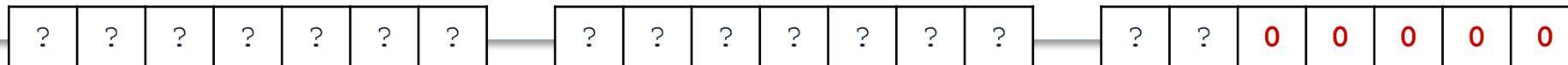
NTHash = MD4 (User Password) – 16 byte value

Challenge Response = DES_{NTHash[1:7]} (ChallengeHash) ||
DES_{NTHash[8:14]} (ChallengeHash) ||
DES_{NTHash[15:21]} (ChallengeHash)

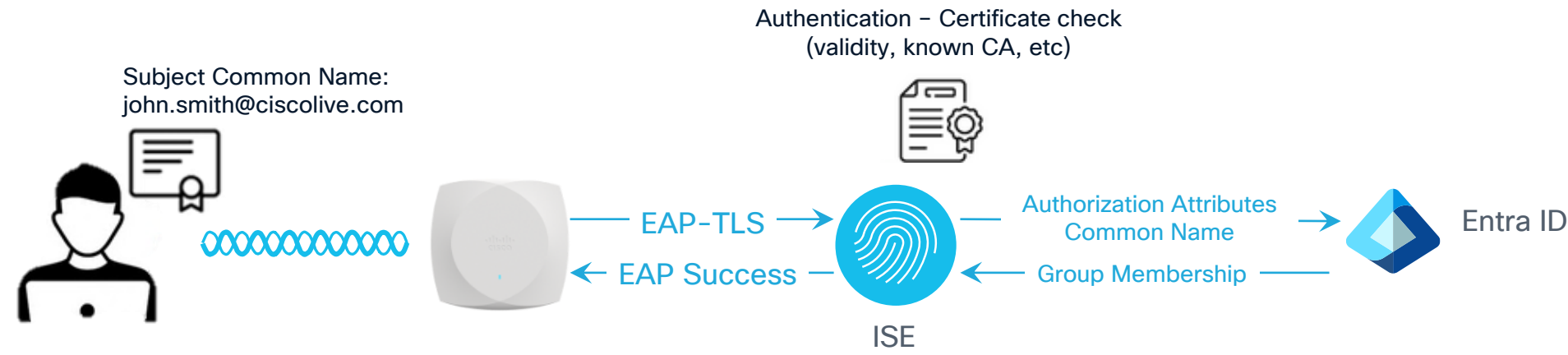
NTHash[1:7]

NTHash[8:14]

NTHash[15:21]



Cloud Identity with EAP-TLS



<https://community.cisco.com/t5/security-knowledge-base/cisco-ise-with-microsoft-active-directory-entra-id-and-intune/ta-p/4763635#toc-hld-76840754>

Apple goto fail Bug

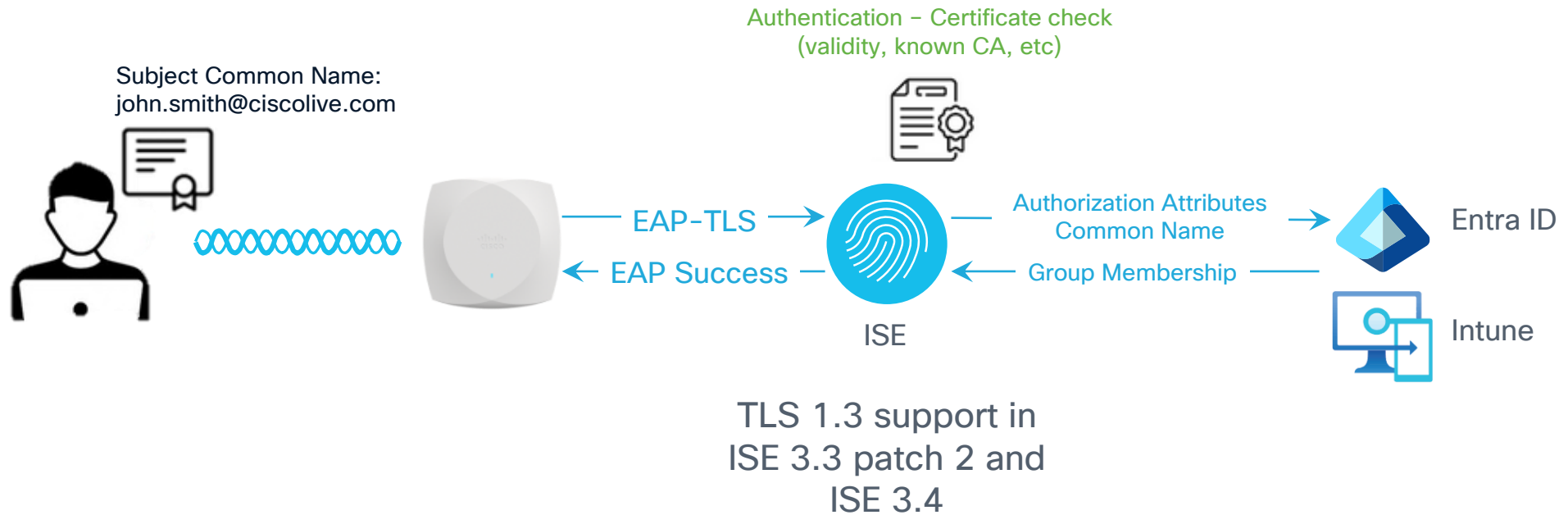
```
static OSStatus
SSLVerifySignedServerKeyExchange(SSLContext *ctx, bool isRsa, SSLBuffer signedParams,
                                uint8_t *signature, UInt16 signatureLen)
{
    OSStatus      err;
    ...

    if ((err = SSLHashSHA1.update(&hashCtx, &serverRandom)) != 0)
        goto fail;
    if ((err = SSLHashSHA1.update(&hashCtx, &signedParams)) != 0)
        goto fail;
        goto fail;
    if ((err = SSLHashSHA1.final(&hashCtx, &hashOut)) != 0)
        goto fail;
    ...

fail:
    SSLFreeBuffer(&signedHashes);
    SSLFreeBuffer(&hashCtx);
    return err;
}
```



Cloud Identity with EAP-TLS



<https://community.cisco.com/t5/security-knowledge-base/cisco-ise-with-microsoft-active-directory-entra-id-and-intune/ta-p/4763635#toc-hld-76840754>

EAP-TLS to RADIUS Fragmentation

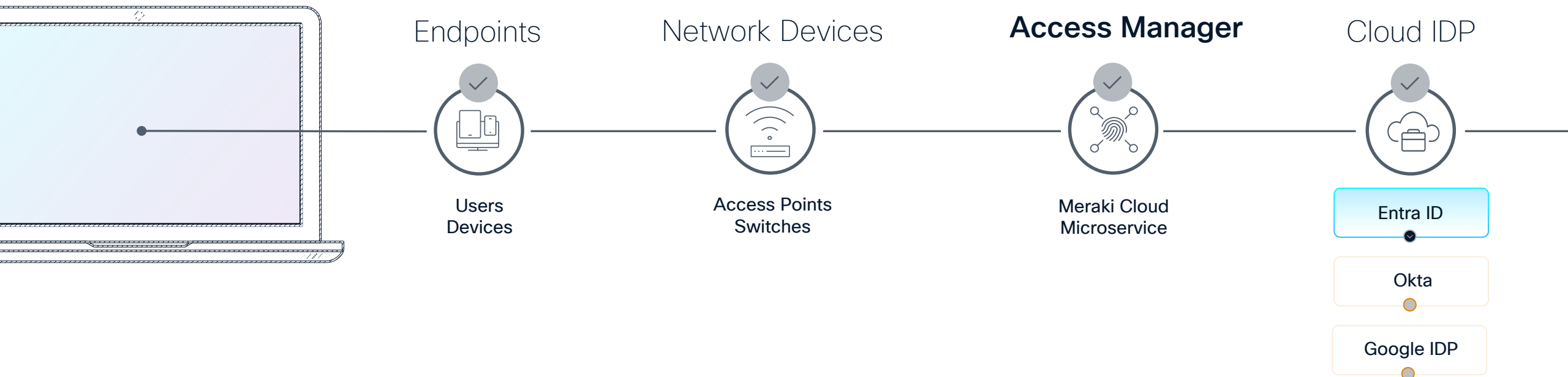


- Potential Solutions:

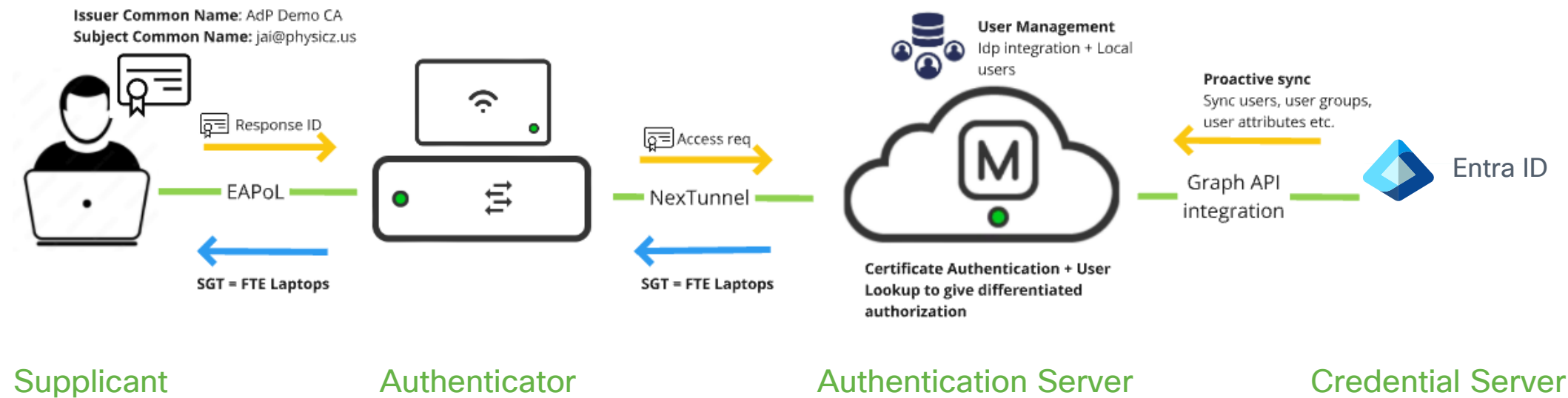
- Add a PSN node local with the WLC
- Enable jumbo packet support on WAN link
- Change firewall rules to handle packet fragmentation



Access Manager



Access Manager and Entra ID with EAP-TLS



Secure Fast Roaming Challenges



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

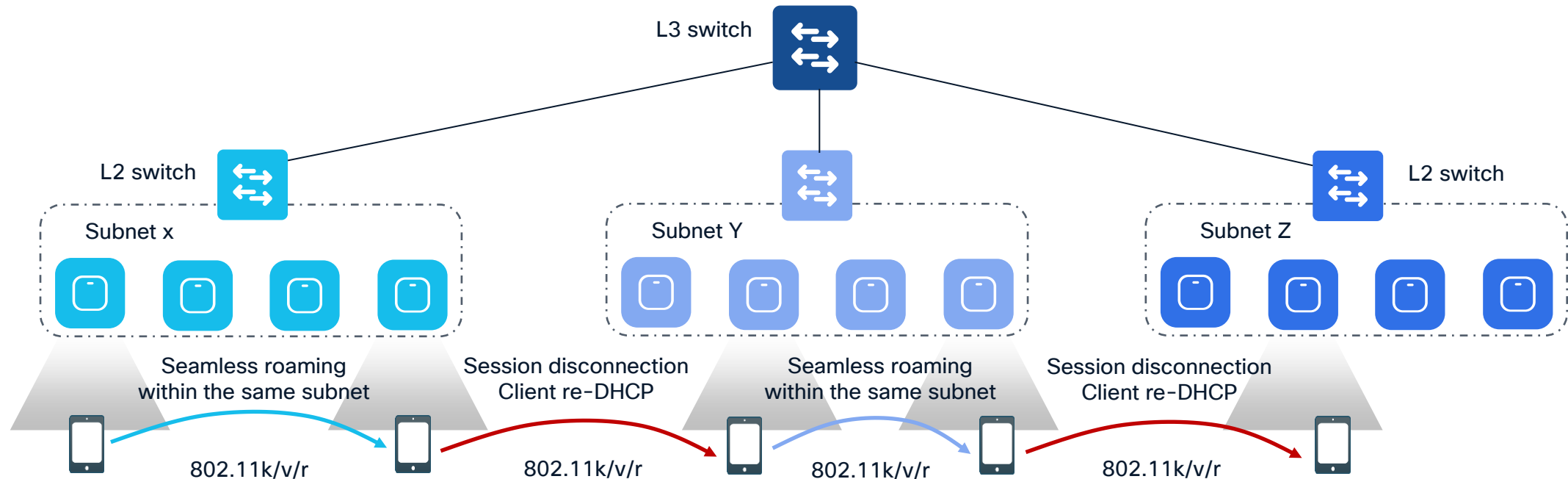


- Client channel scanning and AP selection
 - 802.11k Neighbor Lists based on CCX (Cisco Compatible Extensions)
 - 802.11v BSS Transition
- Re-authentication of client device and re-keying
 - 802.11r Fast BSS Transition based on CCKM (Cisco Centralised Key Management)

Seamless Roaming at Scale

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

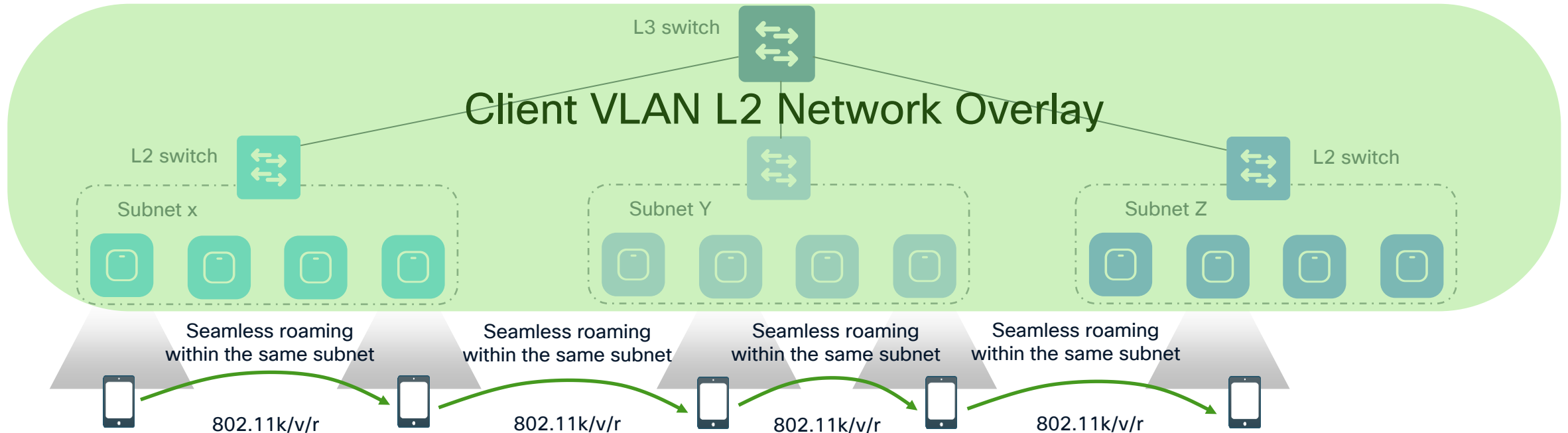
Large broadcast domains do not scale and is counter to networking best practice



Seamless Roaming at Scale

For L3 seamless roaming an extended VLAN network overlay is required

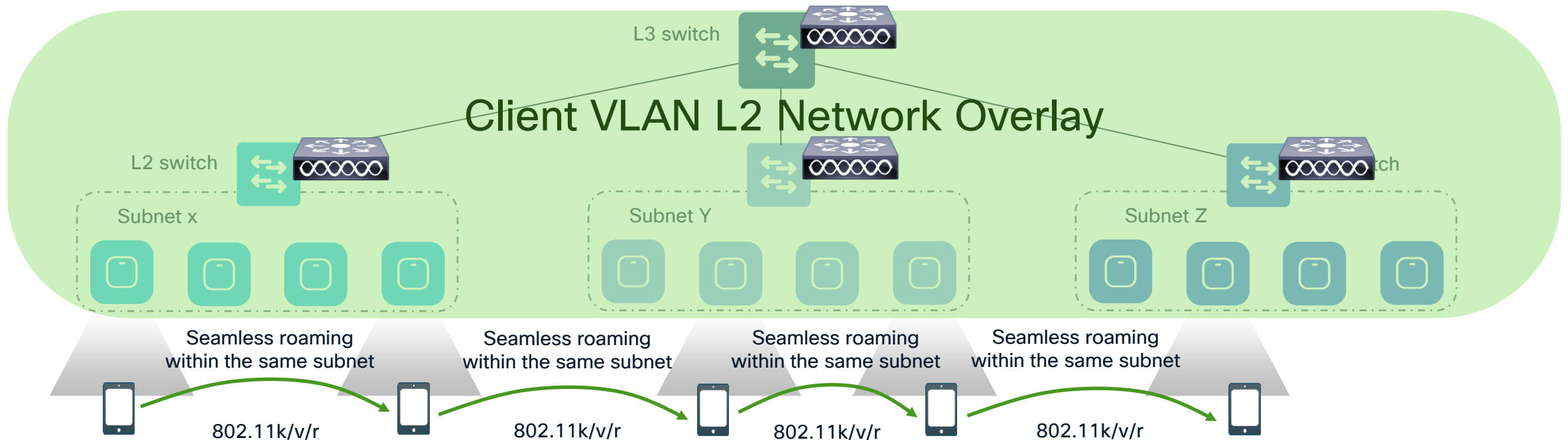
A data termination point is required to roam across L3 boundaries



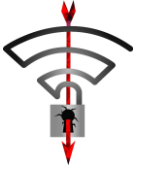
Seamless Roaming at Scale

Edge Wireless Service
Data Plane (DP) Termination

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



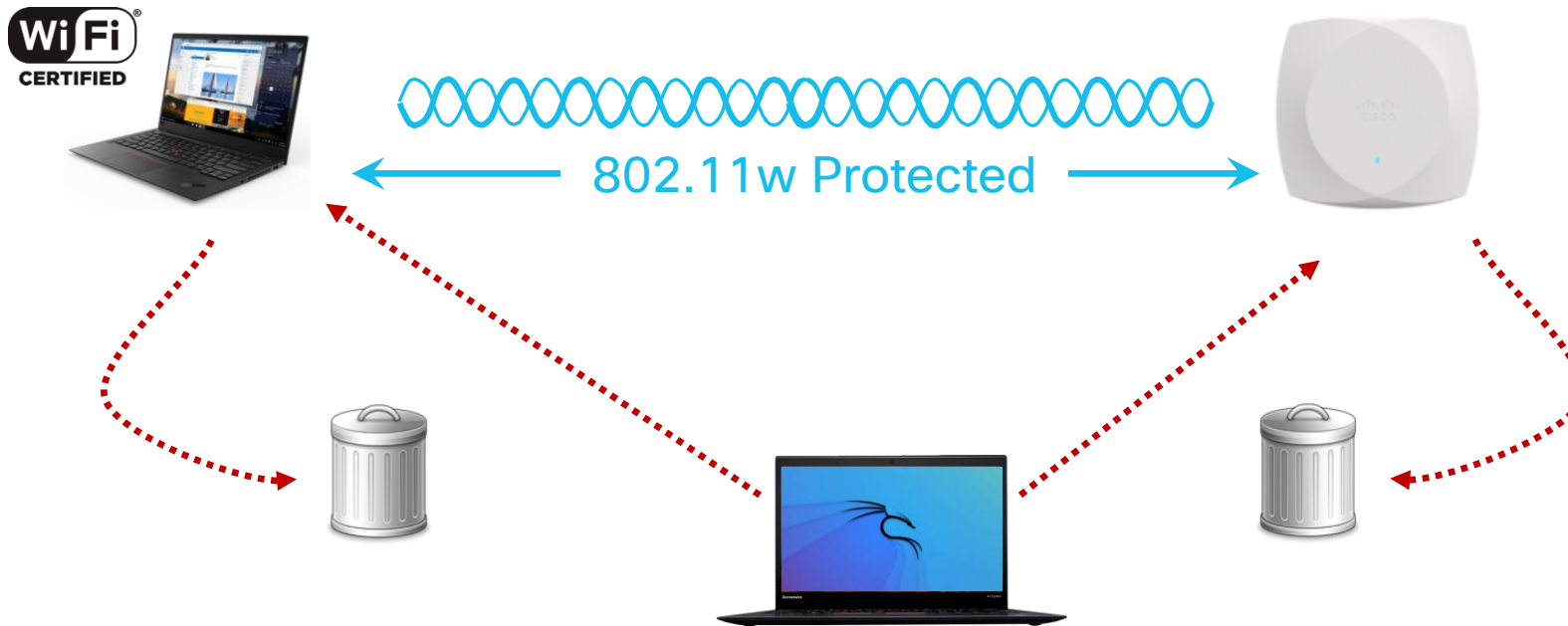
Key Reinstallation Attack



- 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

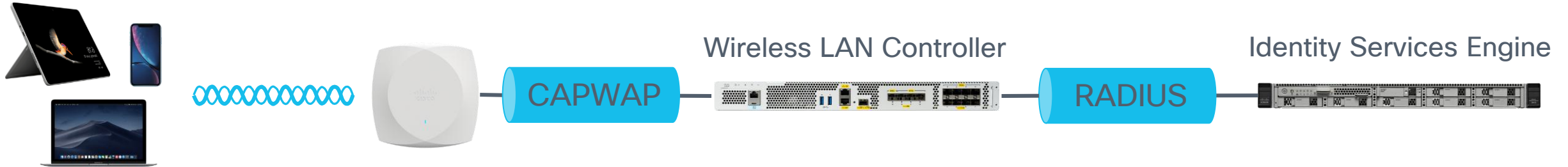
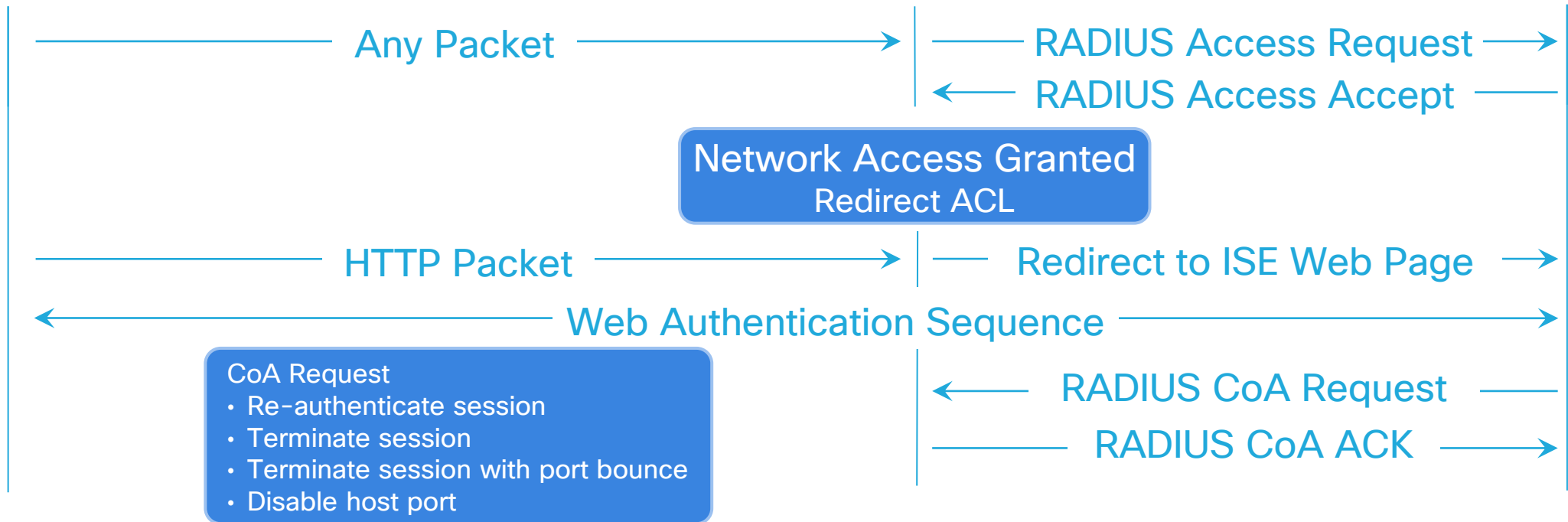
- This was an industry wide issue
 - Not specific to any one vendor
- WPA3 certification includes KRACK exploit testing
- The attacker positions a rogue AP clone to perform a MitM attack
 - This flaw causes all WPA2 encryption protocols to reuse the keystream when encrypting packets
- Rogue AP detection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

802.11w Protected Management Frames



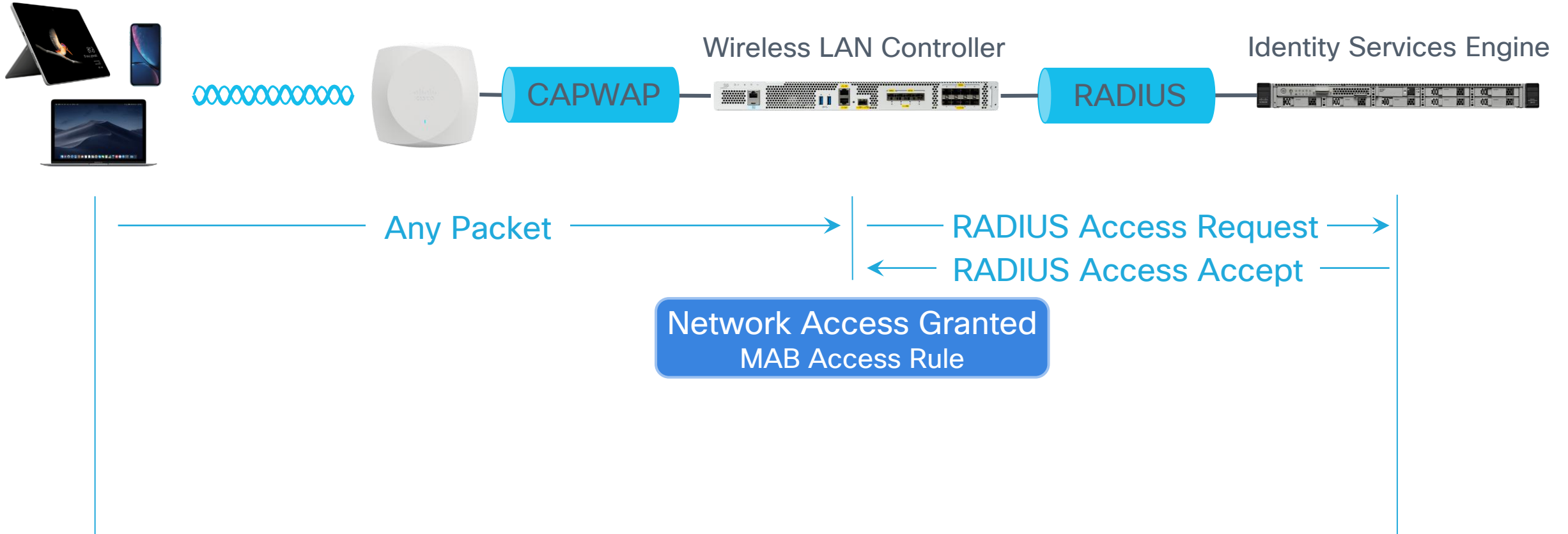
Central Web Authentication

URL Redirect



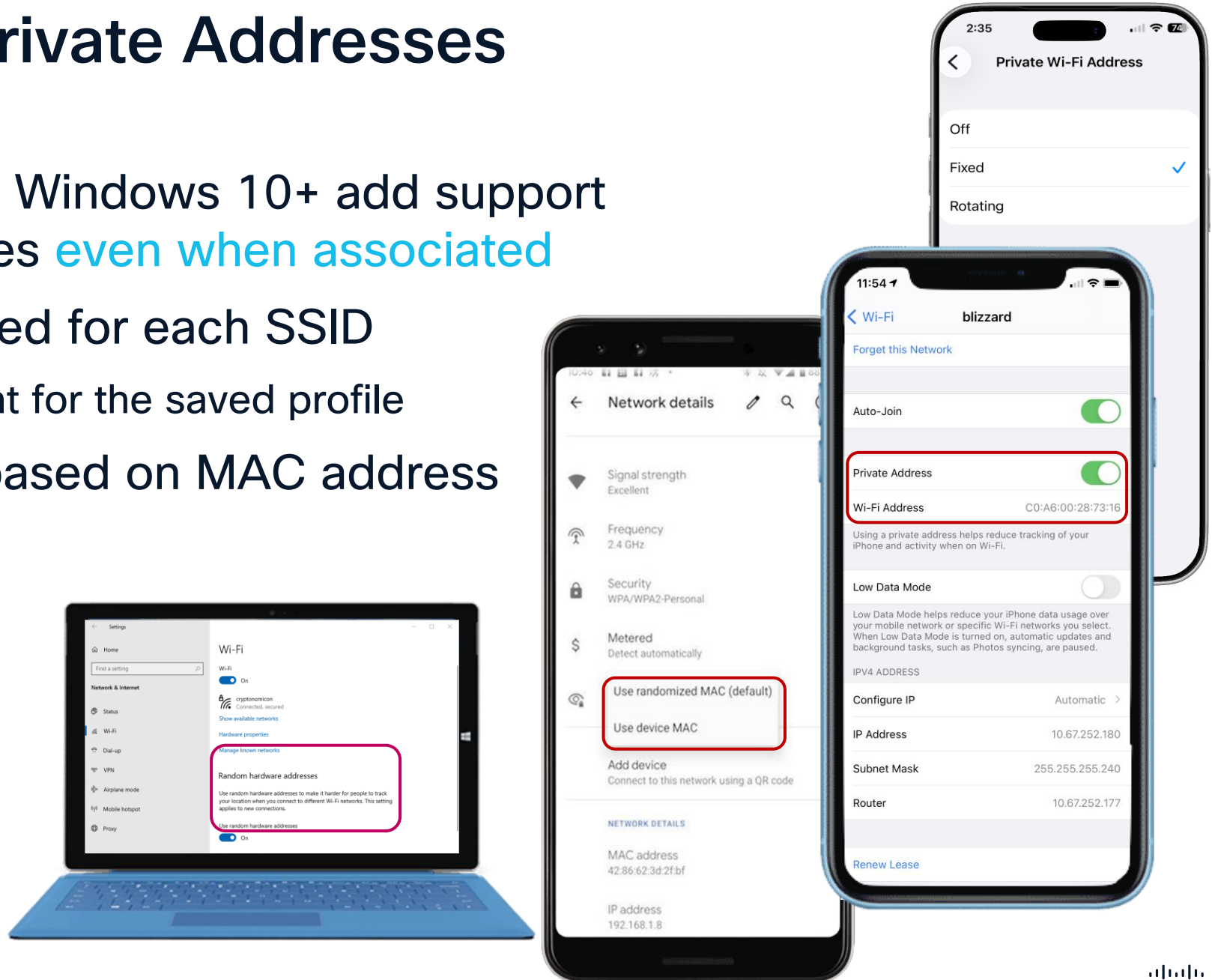
Central Web Authentication

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
 - The MAC **may** remain constant for the saved profile
- This will impact services based on MAC address
 - MAC authentication bypass
 - Web authentication
 - Network troubleshooting
 - Location analytics



Wi-Fi Certified Enhanced Open

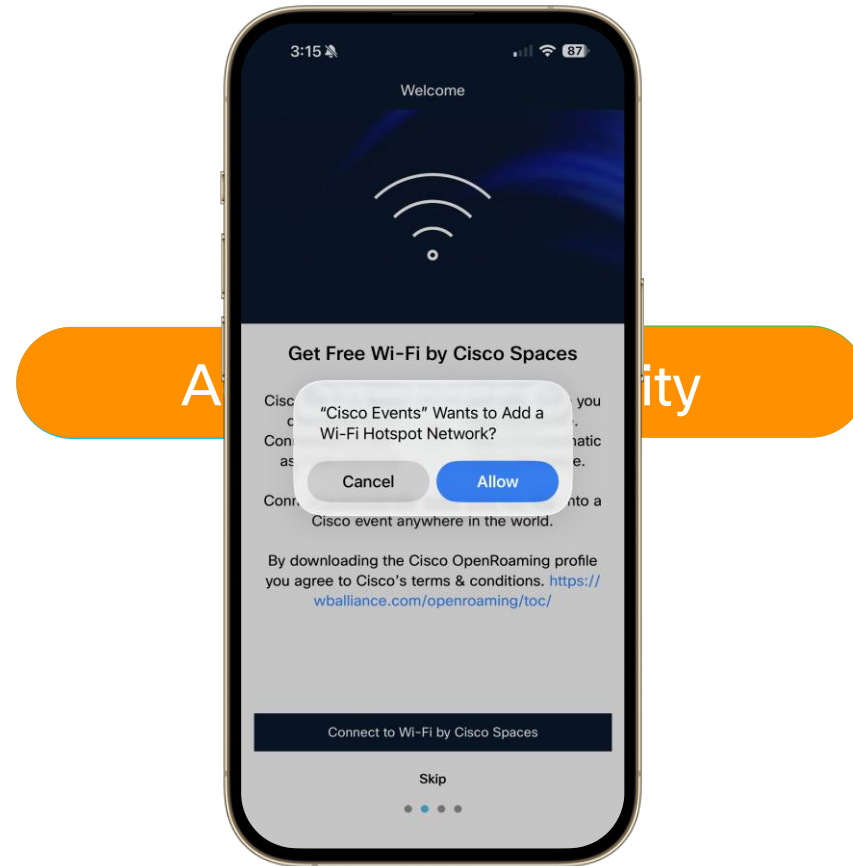
WPA3



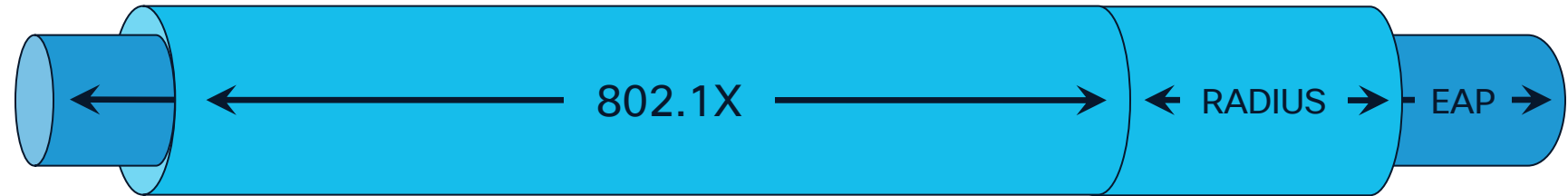
- Opportunistic Wireless Encryption (OWE)
- Reverse "Open" authentication support
- ChaCha20-Poly1305 authenticated Diffie-Hellman Key Exchange to establish a secure session
- Four-Way Handshake to establish a secure session
- Supports Protected Management Frames
- Diffie-Hellman is susceptible to MitM attacks
 - Would allow the attacker same visibility as on an Open network

Man charged over creation of 'evil twin' free WiFi networks to access personal data

Decoupling Access and Identity

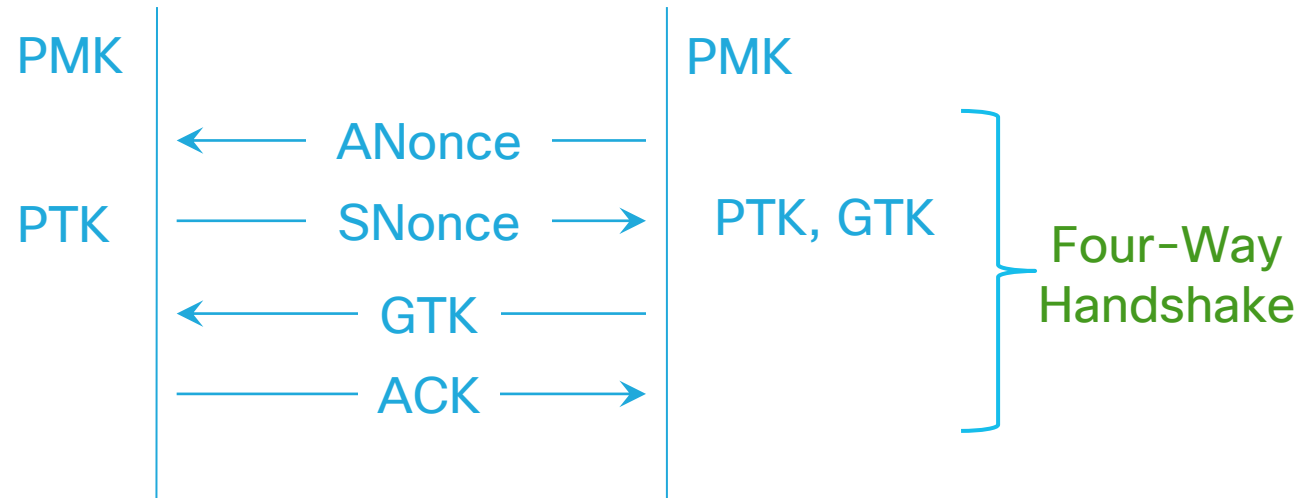


OpenRoaming



WPA Personal

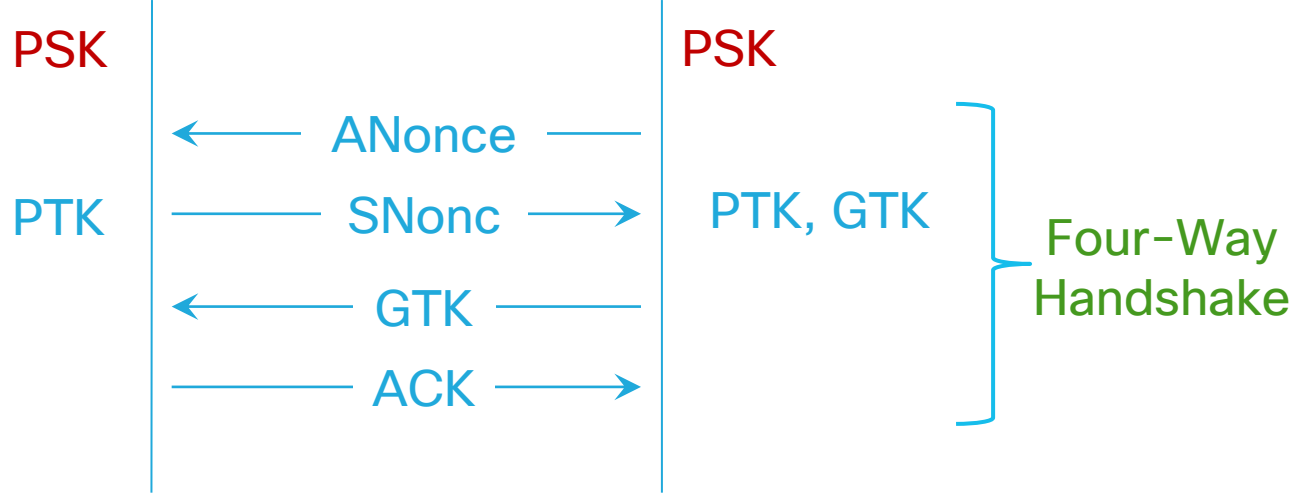
Pre-Shared Key



PTK = SHA(PMK + ANonce + SNonce + AP MAC + STA MAC)

WPA Personal

Pre-Shared Key



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

Time it takes a hacker to brute force your password in 2025

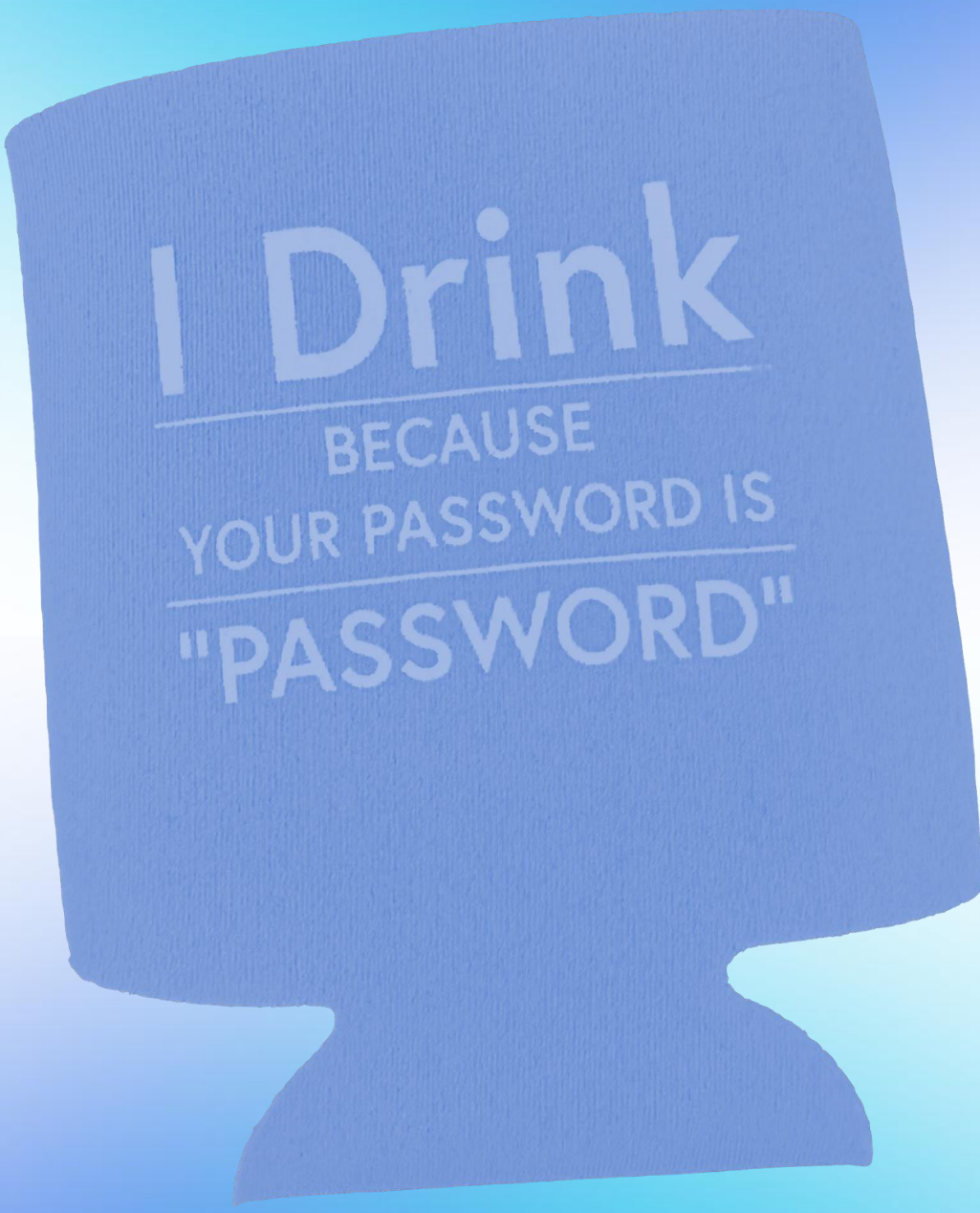
Hardware: 12 x RTX 5090 | Password hash: bcrypt (10)

Number of Characters	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	57 minutes	2 hours	4 hours
6	Instantly	46 minutes	2 days	6 days	2 weeks
7	Instantly	20 hours	4 months	1 year	2 years
8	Instantly	3 weeks	15 years	62 years	164 years
9	2 hours	2 years	791 years	3k years	11k years
10	1 day	40 years	41k years	238k years	803k years
11	1 weeks	1k years	2m years	14m years	56m years
12	3 months	27k years	111m years	917m years	3bn years
13	3 years	705k years	5bn years	56bn years	275bn years
14	28 years	18m years	300bn years	3tn years	19tn years
15	284 years	477m years	15tn years	218tn years	1qd years
16	2k years	12bn years	812tn years	13qd years	94qd years
17	28k years	322bn years	42qd years	840qd years	6qn years
18	284k years	8tn years	2qn years	52qn years	463qn years



Hive Systems

Read more and download at hivesystems.com/password



I Drink
BECAUSE
YOUR PASSWORD IS
"PASSWORD"

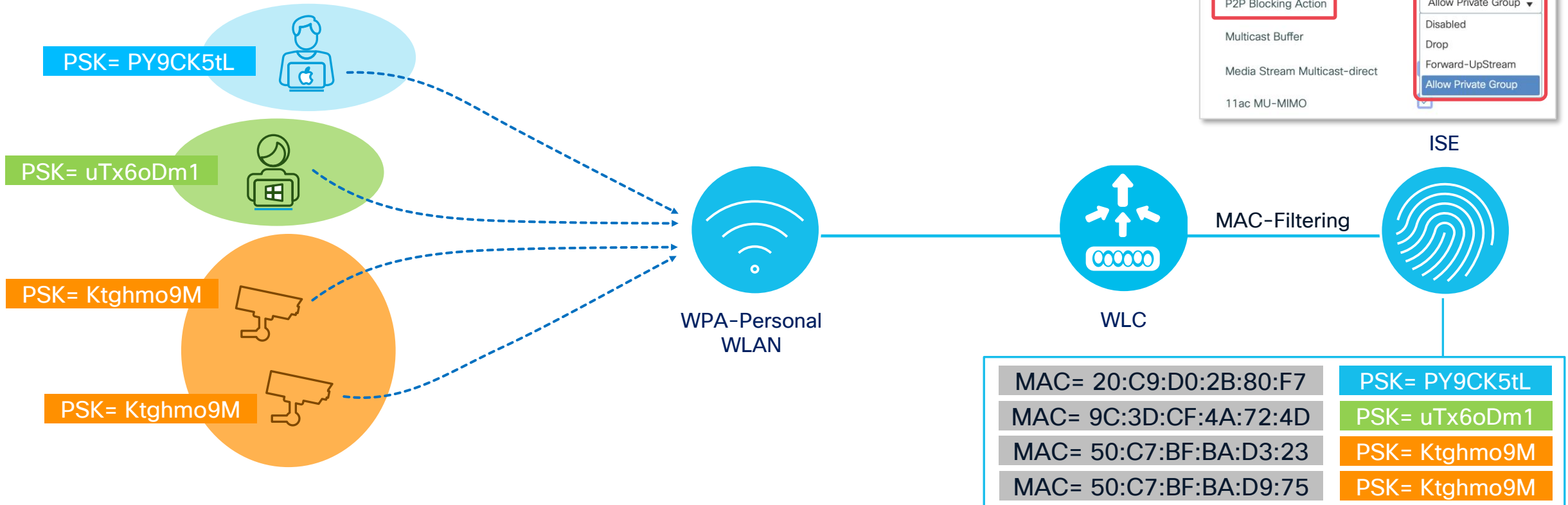
Simultaneous Authentication of Equals

WPA3



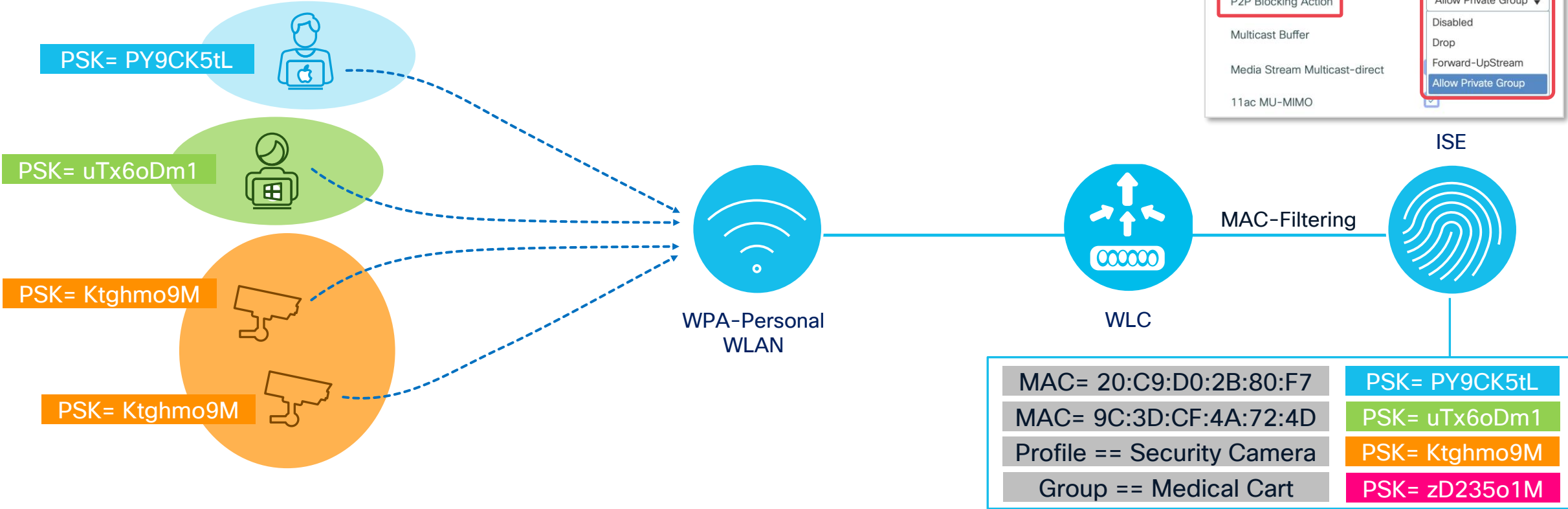
- Based on the Dragonfly Key Exchange
 - Balanced Password Authenticated Key Exchange
 - Security of SAE not tied to the complexity of the shared secret
 - SAE exchanges results in a 32-byte PMK
 - Protects against offline dictionary attacks
 - Forward secrecy protects traffic if the password is compromised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

Identity PSK/SAE



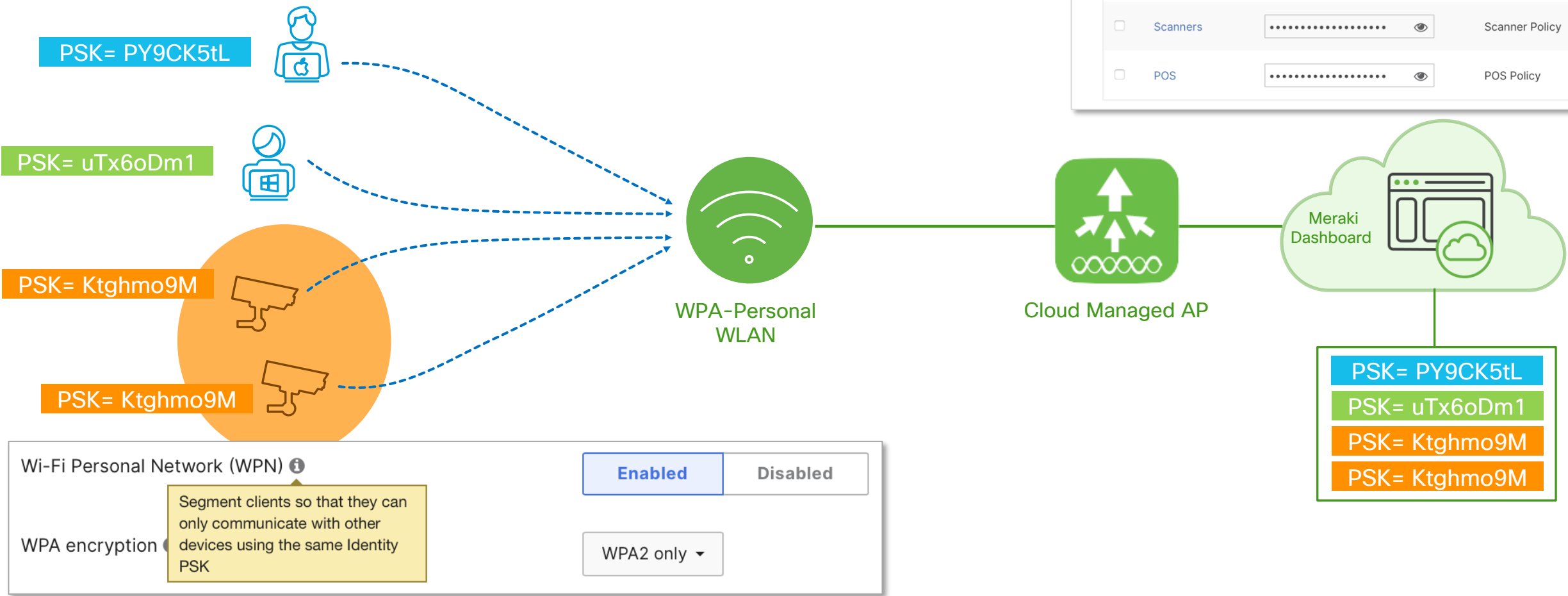
<https://www.cisco.com/c/en/us/support/docs/wireless/catalyst-9800-series-wireless-controllers/216130-configure-catalyst-9800-wlc-ipsec-with-ci.html>
https://documentation.meraki.com/MR/Encryption_and_Authentication/IPSK_with_RADIUS_Authentication

Identity PSK/SAE



<https://www.cisco.com/c/en/us/support/docs/wireless/catalyst-9800-series-wireless-controllers/216130-configure-catalyst-9800-wlc-ipsec-with-ci.html>
https://documentation.meraki.com/MR/Encryption_and_Authentication/IPsec_with_RADIUS_Authentication

Identity PSK without RADIUS

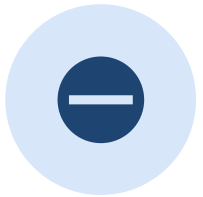


https://documentation.meraki.com/MR/Encryption_and_Authentication/IPSK_Authentication_without_RADIUS

Security Implications of 6GHz



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



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

Catalyst Center

Wireless SSID

Advanced Settings

Configure the advanced fields to complete SSID setup.

SSID Name: WPA2+WPA3-Example (Enterprise)

MFP Client Protection ⓘ

☐ Optional ☐ Required ☒ Disabled

Protected Management Frame (802.11w)

☐ Optional ☒ Required ☐ Disabled

Most secure

User Credentials are validated with 802.1x Radius server to authenticate clients to the wireless network.
WPA3 feature is supported for Wireless Controller version 8.10 & above, For Catalyst 9800 Controllers version 16.12 & above.

802.11b/g Policy

802.11g ▼

☒ Band Select ⓘ

☒ 6 GHz Client Steering

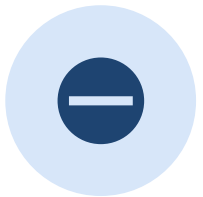
From IOS-XE 17.12.1



Security Implications of 6GHz



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



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

Security

WPA3 Transition Mode Enterprise with 0 RADIUS servers

WPA encryption ⓘ

WPA3 Transition Mode ▾

802.11w ⓘ

☒ Enabled (allow unsupported clients)
☐ Required (reject unsupported clients)
☐ Disabled (never use)

Mandatory DHCP

Enabled

Disabled

Advanced WPA3 settings

(Cipher and AKM suite settings)

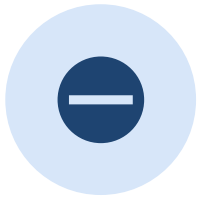
>

From Meraki 31.X

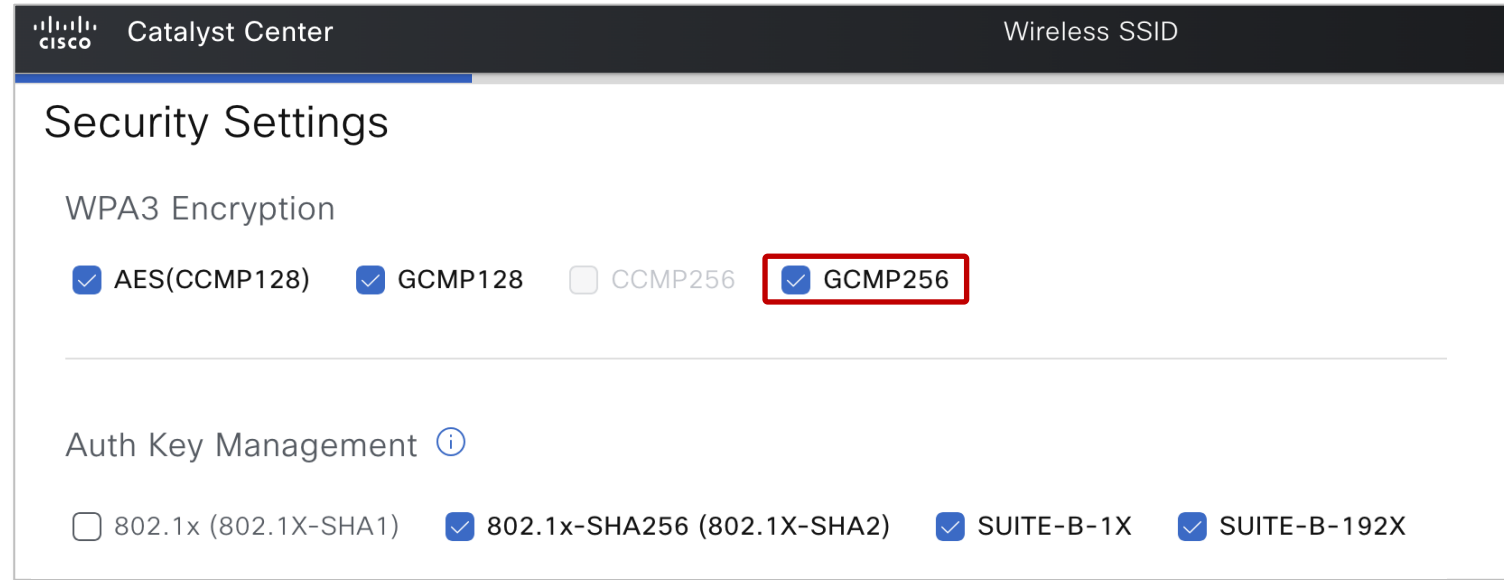
Security Implications of Wi-Fi 7



Wi-Fi 7 brings new AKM and cipher suite requirements



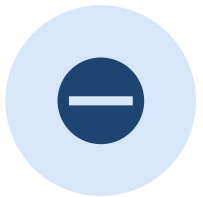
These are **mandatory** for Wi-Fi 7 MCS rates and MLO



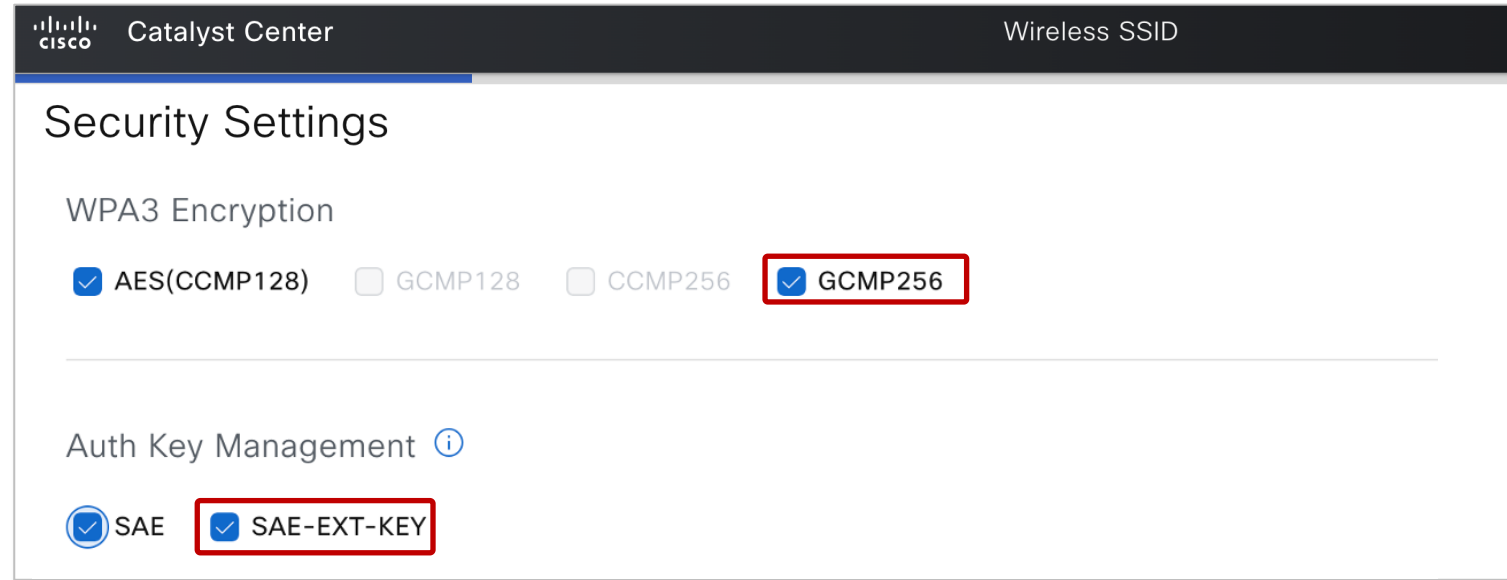
Security Implications of Wi-Fi 7



Wi-Fi 7 brings new AKM and cipher suite requirements



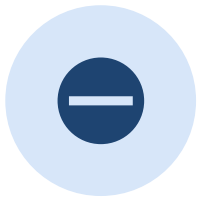
These are **mandatory** for Wi-Fi 7 MCS rates and MLO



Security Implications of Wi-Fi 7



Wi-Fi 7 brings new AKM and cipher suite requirements



These are **mandatory** for Wi-Fi 7 MCS rates and MLO

Security

WPA3 Transition Mode configured

WPA encryption ⓘ

WPA3 Transition Mode ▾

802.11w ⓘ

☐ Enabled (allow unsupported clients)
☒ Required (reject unsupported clients)
☐ Disabled (never use)

Mandatory DHCP

Enabled

Disabled

Advanced WPA3 settings

(Cipher and AKM suite settings)

▾

WPA3 Cipher Suite

☐ GCMP 256

WPA3 AKM Suite

☒ SAE
☐ SAE-EXT

ⓘ

Certain Cipher suite and AKMs are required for capable APs to operate in 802.11be (Wi-Fi 7) mode. Please refer to [documentation](#) for more details.



Wi-Fi 7 requires high wireless security encryption. Selected encryption type does not meet the requirement. Please check [documentation](#) for more details.

Wireless Intrusion Detection and Prevention

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

The screenshot displays the Cisco Catalyst Center interface for Rogue and aWIPS management. The top navigation bar includes 'Assurance / Dashboards / Rogue and aWIPS'. The main content area is divided into two panels. The left panel, titled 'Threats (365)', shows a list of threats with columns for Threat Level, MAC Address, and Type. The right panel, titled 'Threat 360: Mac CE:9C:1E:ED:6D:F0', provides detailed information about a specific threat, including its Threat Level (High), Threat Type (sjc14roguerule), Vendor (UNKNOWN), Status (Active), Containment Status (Open), and Last Reported time (Nov 2, 2024 1:56 PM). Below this, a floor plan map shows the location of the threat (Global/San Jose/Building 14/Floor1) and the detecting AP (SJC14-F1-9164-3). The bottom panel, titled 'Detections (3)', shows a table of detections with columns for Detecting AP, Detecting AP Site, Adhoc, Rogue SSID, Rogue AP MLD MAC, RSSI (dBm), Channels, and Radio Type (Bandwidth).

Threat Level	Threat Type	Vendor	Status	Containment S...	Last Reported
High	sjc14roguerule	UNKNOWN	Active	Open	Nov 2, 2024 1:56 PM

Detecting AP	Detecting AP Site	Adhoc	Rogue SSID	Rogue AP MLD MAC	RSSI (dBm)	Channels	Radio Type (Bandwidth)
SJC14-F1-9164-3	Global/San Jose/Building 14/Floor1	No	thunderstorm	-	-56	149	802.11ax/be(6GHz)

Rogue Detection and Advanced WIPS

- Wireless threat detection
- Forensic capture
- Client exclusion policies

☒ Signature	Default Threshold	Configured Threshold	Time Interval(In Seconds)	Forensic Capture
☒ Association flood	15	Range: 7 - 45 15	1	☒
☒ Authentication Failure Flood	150	Range: 75 - 450 150	10	☐
☒ Authentication flood	15	Range: 7 - 45 15	1	☒
☒ Beacon Flood	30000	Range: 15000 - 90000 30000	10	☐
☒ Block Ack Flood	1000	Range: 500 - 3000 1000	10	☐
☒ Broadcast probe	1000			

aWIPS and Forensic Capture Enablement

☒ aWIPS ? ☒ Forensic Capture ?

Catalyst Center Assurance / Dashboards / Rogue and aWIPS

Overview Threats Allowed List Rules aWIPS Profile

Site: Global

Threats (365)

Threat Level Threat Level Threat Level

High High High

MAC Address MAC Address MAC Address

D9:55:CA:90:4D:B0 81:DB:3B:D4:AC:C1 6E:49:82:7A:48:A0

Type Type Type

Fuzzed Bea Fuzzed Bea Fuzzed Bea

Threat Type

Malformed Authentication Invalid MAC OUI Authentication Failure Flood Malformed Association Request Airdrop Session Block Ack Probe Response

Malformed authentication request which can trigger bugs in peer networks being dynamically c Invalid MAC OUI. Authenticatio Malformed association request is invalid, unexpected or random data is introduced in the probe request and then replaying those modified frames into the air. Airdrop session is when Apple feat file sharing. This could potentially peer networks being dynamically c

CTS Flood

CTS Flood attack is when specific device send a bulk CTS control packet to wireless devices sharing same RF medium and it will block wireless devices from using RF medium until CTS flood stops.

RTS Flood

RTS Flood attack is when specific device send a bulk RTS control packet to AP for blocking wireless bandwidth that leads to performance disturbance for clients on that AP.

EAPOL logoff flood

EAPOL- logoff flood is when a specific device tries to send Extensible Authentication Protocol over LANs (EAPOL) logoff packets, which are used in the WPA and WPA2 authentication for Denial of Service (DoS).

Deauthentication broadcast

Deauthentication Broadcast is when a specific device tries to send a de-authentication frame from the access point to the broadcast address. This de-authenticates all clients.

Deauthentication flood

Deauthentication flood is when an attacker attempts to bring down an access point by flooding it with EAPOL-Start frames to exhaust the access point internal resources

Disassociation broadcast

Disassociation broadcast is when a potential hacker spoofs the MAC address of the wireless client and sends out a flood of PS-Poll frames. The access point then sends out the buffered data frames to the wireless client leading to client missing the data frames since it could be in the power save mode.

Disassociation flood

Disassociation flood is when a potential hacker spoofs the MAC address of the wireless client and sends out a flood of PS-Poll frames. The access point then sends out the buffered data frames to the wireless client leading to client missing the data frames since it could be in the power save mode.

EAPOL-Start V1 Flood

EAPOL start flood is when an attacker attempts to bring down an access point by flooding it with EAPOL-Start frames to exhaust the access point internal resources

PS Poll Flood

PS poll flood is when a potential hacker spoofs the MAC address of the wireless client and sends out a flood of PS-Poll frames. The access point then sends out the buffered data frames to the wireless client leading to client missing the data frames since it could be in the power save mode.

Fuzzed Probe Response

Fuzzed Probe Response is when invalid, unexpected or random data is introduced in the probe response and then replaying those modified frames into the air.

Fuzzed Probe Request

Fuzzed Probe Request is when invalid, unexpected or random data is introduced in the probe request and then replaying those modified frames into the air.

Fuzzed Beacon

Fuzzed Beacon is when invalid, unexpected or random data is introduced in the beacon This can cause unexpected es, operating system crashes in of arbitrary code on the of attacks (Track by Pair) for

General

Client Exclusion Policies

☒ Excessive 802.11 Association Failures.

☒ Excessive 802.1X Authentication Failures.

☒ Excessive 802.1X Authentication Timeout.

☒ IP Theft or IP Reuse.

☒ Excessive Web Authentication Failures.

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 key

Rogue Detection and Configuration

Detect Access Points that have been installed on a secure network without explicit authorization from a system administrator and configure rogue general configuration parameters



Rogue Detection

Minimum RSSI (dBm)*

-90

Value should be in range -128 and -70.

Transient Interval (seconds)*

0

Value should be 0 or from 120 to 1800.

Report Interval (seconds)*

10

Value should be in range 10 and 300.

General

Client Exclusion Policies

Rogue Detection Security Level.

CUSTOM

Expiration timeout for Rogue APs (seconds).

1200



Validate Rogue Clients against AAA.



Validate Rogue APs against AAA.

Rogue Polling Interval (seconds).

3600



Detect and Report Adhoc Networks.

Rogue Detection Client Number Threshold.

0

Rogue Init Timer (seconds).

180

AP Authentication Alarm Threshold.

1

Allowed List

AP MAC addresses that are in the allowed list are known AP and so are not considered as malicious.

Friendly

Friendly APs belong to one wireless controller and are seen as a Rogue AP by another wireless controller, where both wireless controllers are managed by Catalyst Center.

Neighbor

Neighbor APs are Rogue APs with signal strength less than or equal to -75dBm and are not broadcasting any corporate SSIDs.

Cisco Catalyst Centre Threat Levels

Informational

- RSSI ≤ -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 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

Add Rogue General Configuration

This capability allows to configure Rogue general configuration and client exclusions policies.

Design Name*

Lock all ⓘ

General

Client Exclusion Policies

Rogue Detection Security Level.

CUSTOM

ⓘ

Expiration timeout for Rogue APs (seconds).

Validate Rogue Clients against AAA.

ⓘ

Validate Rogue APs against AAA.

ⓘ

Rogue Polling Interval (seconds).

Detect and Report Adhoc Networks.

ⓘ

© 2025 Cisco and/or its affiliates. All rights reserved.

BRKEWN-2104

 CISCO

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 is critical

The screenshot displays the Cisco Meraki Threat Detection interface. The top section shows a threat summary for 'Threat 360: Mac A4:53:0E:7C:99:E0' with a 'High' threat level and 'HoneyPot' threat type. Below this, a 'Warning' dialog box is visible, stating: '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'. The main table lists threats, with 'Threat 360: Mac C6:9E:38:75:52:D8' highlighted. This threat is categorized as 'Potential' with a threat type of 'Interferer' and a status of 'Active'. The containment status is 'Open'. Below the table, the location is specified as 'Global/San Jose/Building 14/Floor1'. A floor plan diagram shows the physical layout of the building, with various access points (APs) and switches labeled. A red circle highlights a specific area on the floor plan, likely indicating the location of the rogue AP. The interface also includes a sidebar with a list of devices and their status.

Threat Level	Threat Type	Vendor	Status	Containment S...	Last Reported
High	HoneyPot	Cisco Systems, Inc	Active	Open	Jun 1, 2022 02:48 pm
Potential	Interferer	UNKNOWN	Active	Open	Jun 4, 2022 06:23 pm

Rogue Containment with WPA3

Threat 360: Mac C6:9E:38:75:52:D8

Threat Level

Threat Type

Vendor

Status

Containment S...

Actions

Potential

Interferer

UNKNOWN

Active

Open

Last Reported

Jun 4, 2022 06:23 pm

Location: Global/San Jose/Building 14/Floor1

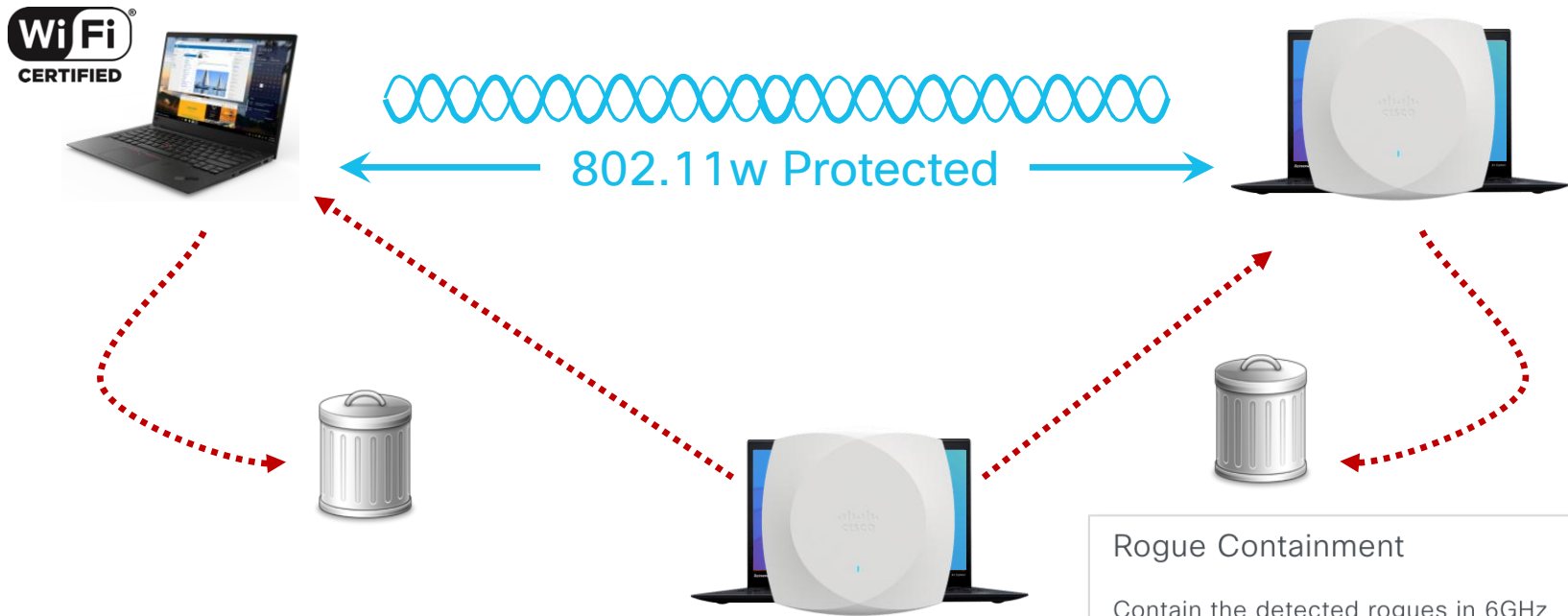
Full Screen

WS-C3850-48PTME_Switch

SJC14F1-WTME-C9K-48UXM.cisco.com

#1

#1



Rogue Containment

Contain the detected rogues in 6GHz

☐

PMF Denial ⓘ

PMF Denial is supported from IOS-XE version 17.12 and above

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 aWIPS (Advanced Wireless Intrusion Prevention System) interface. The left sidebar shows the 'Overview' tab with a 'High Threat Summary' section indicating 14 active high threats, categorized by threat type (Top 10 and All). Below this is a 'Threats (134)' table listing various threats, including 'Rogue on wire' threats with their MAC addresses and threat levels.

The main content area shows a detailed view of a specific threat: 'Threat 360: Mac 6A:3A:0E:53:A6:E9'. This threat is classified as 'High' and is a 'Rogue on wire' type. The interface includes a map showing the location of the threat (Global/San Jose/Building 14/Floor1) and a list of detected devices, including 'WS-C3850-48PTME_Switch' and 'SJC14F1-WTME-C9K-48UXM.cisco.com'. The 'Switch Port Detail' section shows the host MAC address (70:F3:5A:7B:9F:71) and the device name (WS-C3850-48PTME_Switch) connected to the interface GigabitEthernet5/0/47.

Key interface elements include:

- Threat Level:** High
- Threat Type:** Rogue on wire
- Vendor:** UNKNOWN
- Status:** Active
- Containment Status:** Open
- Actions:** Shutdown Switchport, Add to Allowed list
- Location:** Global/San Jose/Building 14/Floor1
- Switch Port Detail:** Host Mac: 70:F3:5A:7B:9F:71, Device Name: WS-C3850-48PTME_Switch, Device IP: 172.20.224.156, Interface Name: GigabitEthernet5/0/47, Last Updated: 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
- Rogue detection support has been extended beyond the regulatory domain of the network
 - Alerts are generated for rogue APs broadcasting on unauthorized 2.4 and 5 GHz radio channels

From MR 31.X

Air Marshal

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

24 rogue SSIDs ¹ seen for the last 2 hours ▾

Edit ▾ Search...

☐	SSID ▲	Broadcast MACs	Last seen	First seen	Containment	Rogue because	
☐	AXE BLE testing	6e:3a:0e:ff:f8:f5 (and 1 other)	4 seconds ago	1 year ago	🟡 partial	Recently seen on LAN	
☐	IT Test WiFi	e0:cb:bc:49:35:61 (and 1 other)	50 seconds ago	1 month ago	🟢 contained	Recently seen on LAN	
☐	j-bond-2-owe	c6:14:92:6e:ae:b2 (and 2 others)	15 seconds ago	2 months ago	🟡 partial	Recently seen on LAN	
☐	j-bond-3-sae	ca:14:a2:6e:ae:b0 (and 1 other)	15 seconds ago	3 weeks ago	🟡 partial	Recently seen on LAN	
☐	j-bond-5-1x	c6:14:92:6e:ae:a5 (and 4 others)	6 seconds ago	3 weeks ago	🟡 partial	Recently seen on LAN	
☐	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	
☐	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	
☐	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	
☐	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	
☐	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:49:35:61](#) [e2:cb:ac:49:35:61](#) [e0:cb:bc:49:35:61](#)

Wired MACs [e0:cb:bc:49:35:61](#)

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)

Network as a Sensor and Enforcer

Network as a Sensor

Secure Network Analytics Integration



Malware detection and cryptographic compliance with Secure Network Analytics

Secure Network Analytics

IT-Data Store

Monitor

Investigate

Report

Configure

Apps

Alarming Hosts

Concern Index 0 Target Index 0 Recon 0 C&C 0 Exploitation 0 DDoS Source 0 DDoS Target 0 Data Hoarding 0 Exfiltration 0 Policy Violation 1 Anomaly 1

Top Alarming Hosts

Host 10.10.100.63 End User Devices Category AN

Alarms by Type

Event Count 400 357 221 166 161 28

Today's Alarms

Policy Violation 1 Anomaly 1

Flow Collection Trend

Flow Count 2000 1000 0 10:00 PM 11:00 PM 12:00 AM 1:00 AM 2:00 AM

Top Applications

HTTP 1.0% HTTP 0.5% HTTP 0.5% HTTP 0.5% HTTP 0.5% HTTP 0.5% HTTP 0.5% HTTP 0.5% HTTP 0.5% HTTP 0.5%

Alerts

Search Start End Filter by time range (UTC) Reset Apply

See alerts by status: Open Snoozed Unpublished Closed All

Persistent Remote Control Connections

Alert

Description Device is receiving persistent connections from a new host on a remote control protocol like Remote Desktop or SSH. This may indicate that a firewall rule or ACL is overly permissive.

Next Steps Adjust firewall or security group rules to prevent malicious attempts to repeatedly access the entity. Confirm that the local entity has not been breached by checking the supporting evidence or the entity.

MITRE Tactics Initial Access

MITRE Techniques External Remote Services

Alert Type Priority Normal (Default) Go to alert priorities page

ETA Cryptographic Audit

Type of Report Audit Report

Time Range Start Time 01 November 2025 00:00 End Time 02 November 2025 20:30

Subject Host Groups DMZ Servers

Peer Host Groups Inside Hosts Outside Hosts

Audit Results

November 1, 2025 00:00 - November 2, 2025 20:30

Subject Orientation: Server

Subject Host Groups: DMZ Servers

Peer Host Groups: Inside Hosts Outside Hosts

Download Report Download CSV

Summary View

Filter: Start typing, click anywhere in a chart or click on its respective legend to add a filter tag.

TLS

Version Percent 69 MB 753 KB

Cipher Suite

TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 80.50%

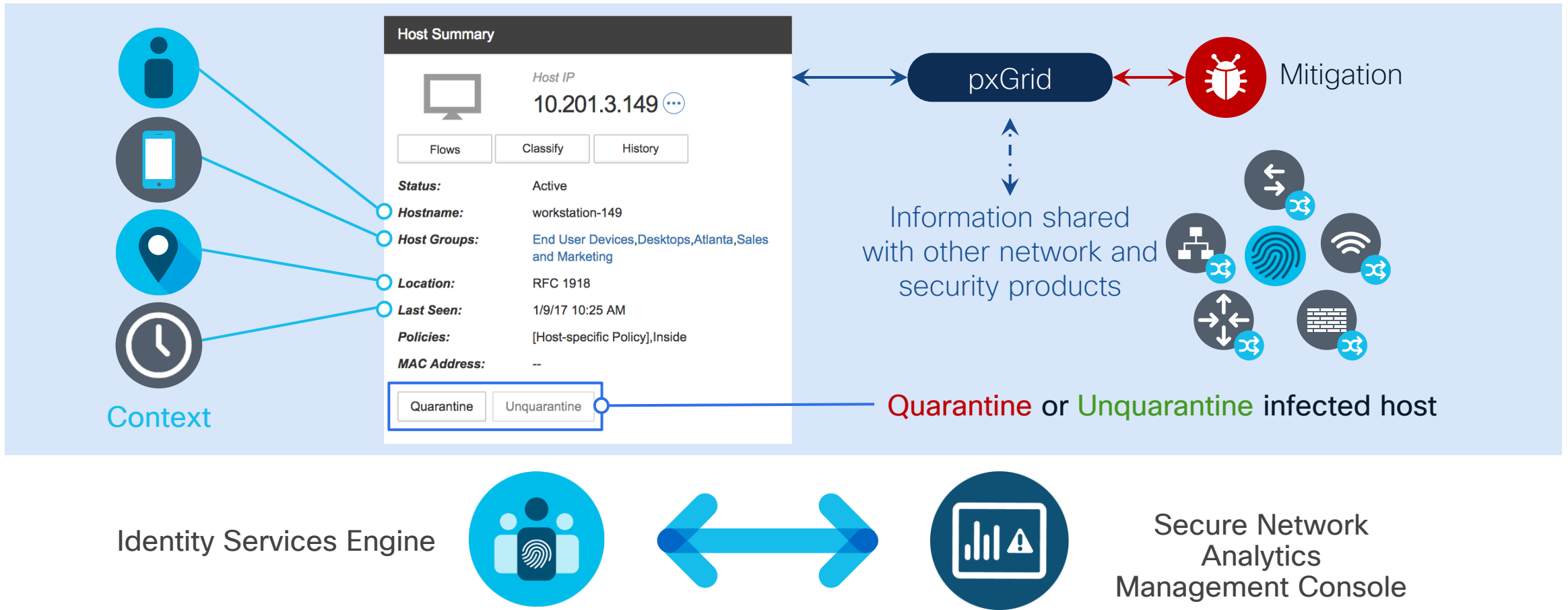
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 37.50%

TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 12.50%



Network as an Enforcer

Rapid Threat Containment



10:01

Thursday, April 18



Securing the Wireless Network



Secure the Air



Secure the Devices



Secure the Network



Thank you

CISCO Live !

Continue your education



Visit the Cisco Stand for related demos



Book your one-on-one Meet the Expert meeting



Attend the interactive education with Capture the Flag, and Walk-in Labs



Visit the On-Demand Library for more sessions at www.CiscoLive.com/on-demand

Complete your session evaluations



Complete a minimum of 4 session surveys and the Overall Event Survey to claim a Cisco Live T-Shirt.



Earn up to 800 points by completing all surveys and climb the Cisco Live Challenge leaderboard.



Level up and earn exclusive prizes!



Complete your surveys in the Cisco Live Events app.

