

CISCO *Live!*

Let's go

#CiscoLive



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

@mkrisch

BRKEWN-3004

CISCO *Live!*

#CiscoLive

Abstract

This session will explore secure wireless network design, with a key focus on the latest WPA3 and Wi-Fi 6 standards. Mobility brings unique challenges to network security, such as the need for secure fast roaming. Participants will learn how 802.11 addresses these requirements, and explore the changes WPA3 brings and the implications for wireless deployments. We will also address specific scenarios such as BYOD, Cloud Identity Providers and Zero Trust.

This session will also explore how Cisco DNA Center expands upon the wireless security standards with Rogue AP detection and location, and Advanced Wireless Intrusion Detection and Prevention, including upcoming capabilities. The intent is to provide a deeper understanding, not just about the security capabilities themselves, but to do so from the perspective of the attacks that they defend against.

Cisco Webex App

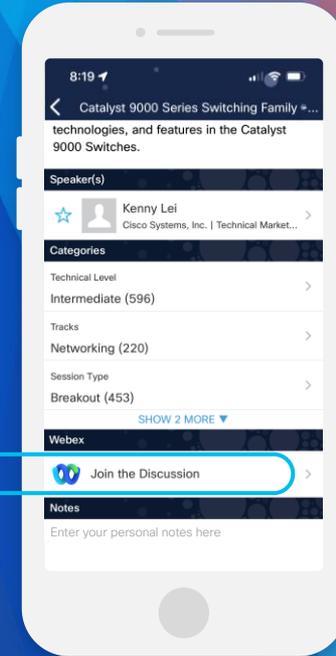
Questions?

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 June 9, 2023.



<https://cislive.ciscoevents.com/cislivebot/#BRKEWN-3004>

Agenda

- Wireless Security Fundamentals
 - WPA3
 - Authentication and Authorization
 - Wi-Fi 6E Security
- Rogue Detection and Advanced WIPS
 - Threat 360°
 - Rogue Detection and Containment
 - Advanced Wireless Intrusion Prevention



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



Secure the
Air



Secure the
Devices



Secure the
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)

WPA3

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

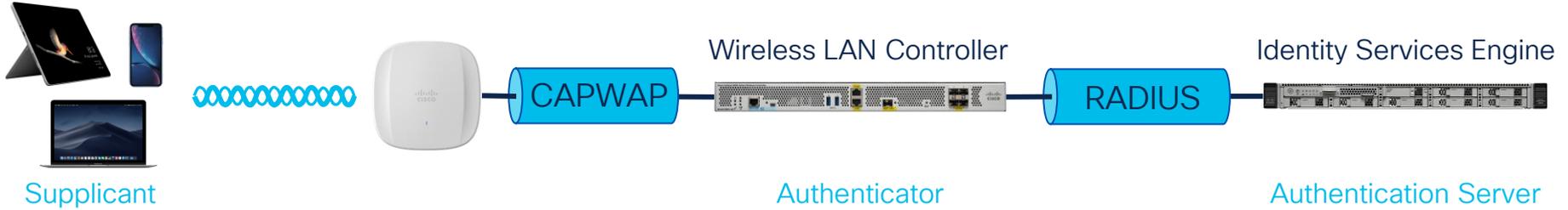


WPA3

- 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)

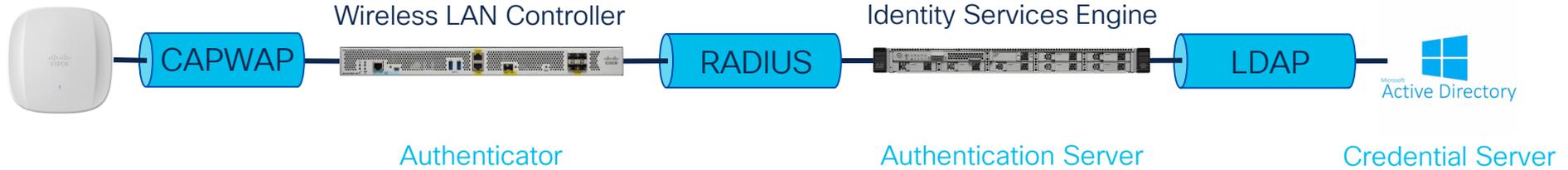
802.11 Fundamentals

Authentication



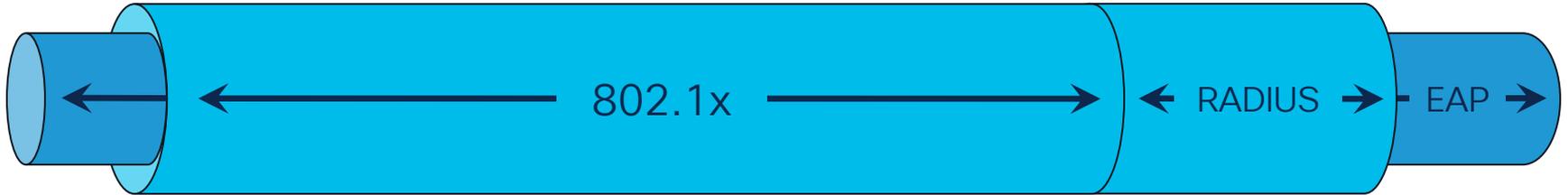
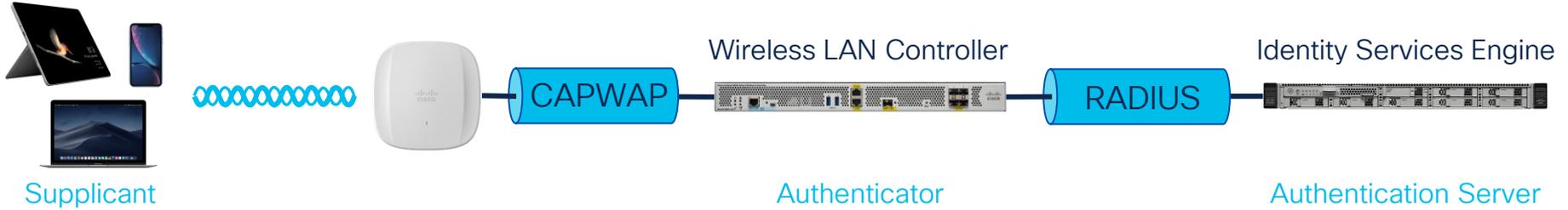
802.11 Fundamentals

Authentication



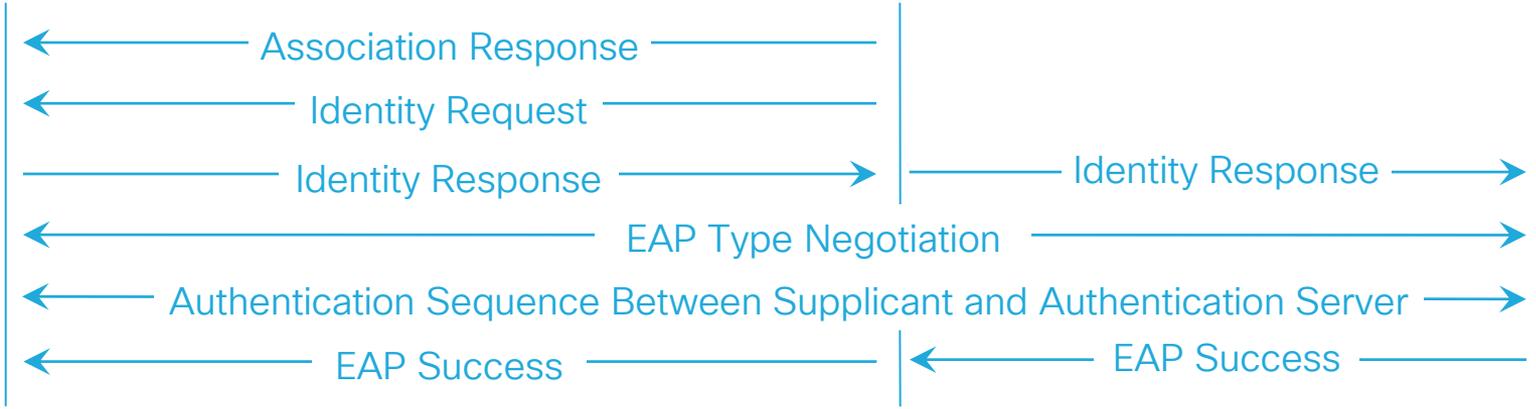
802.11 Fundamentals

Authentication



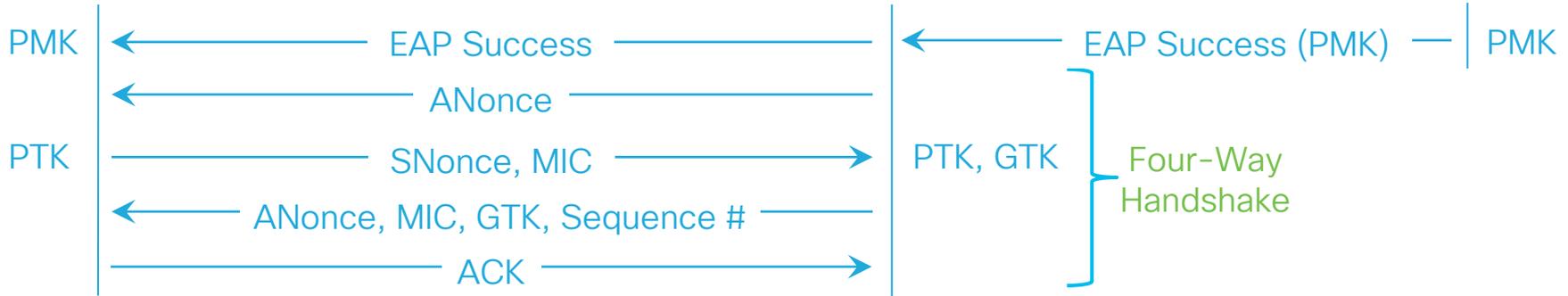
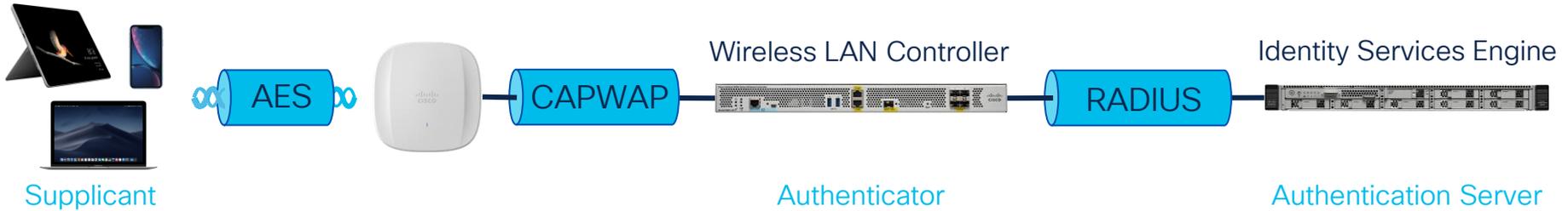
802.11 Fundamentals

Authentication



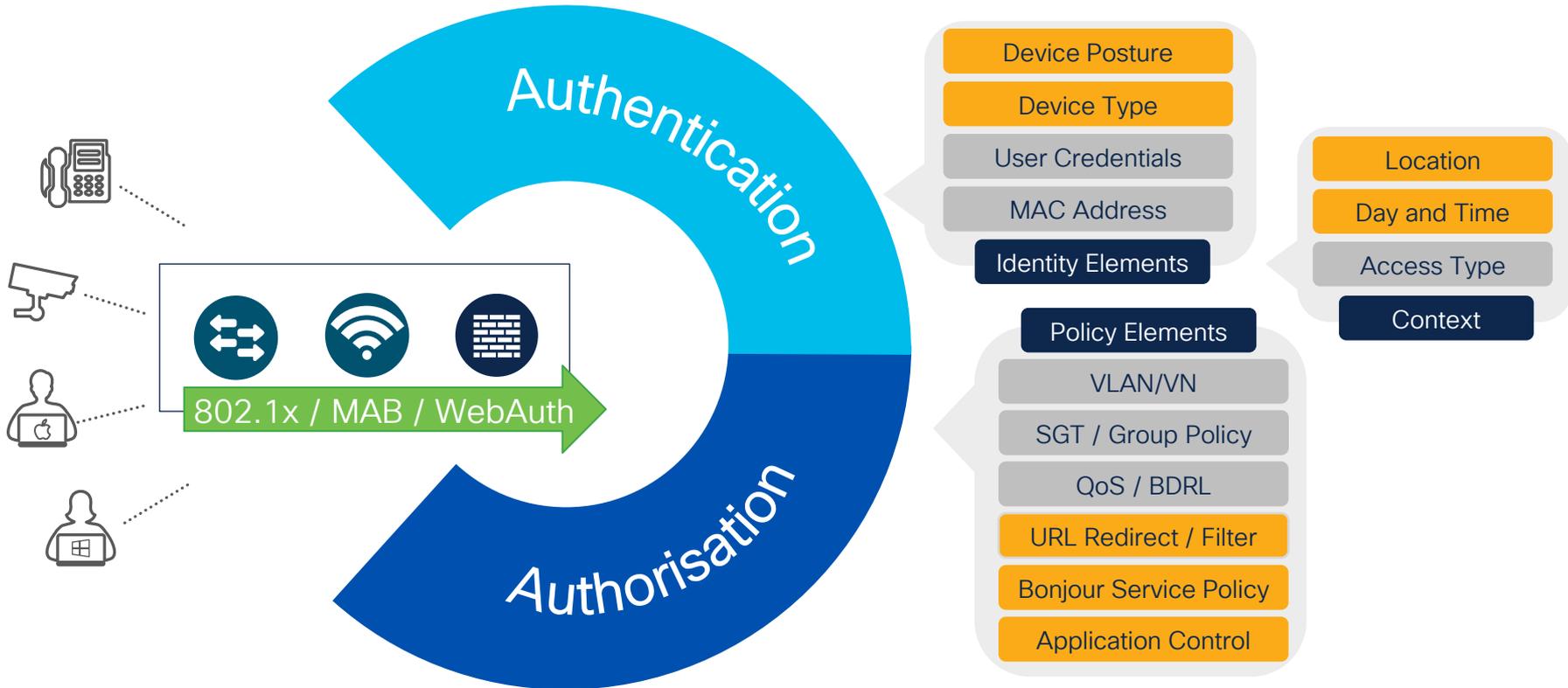
802.11 Fundamentals

Encryption



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

Authentication and Authorisation



Authorization Options



URL-Redirect

Provide conditional web redirect when traffic is blocked



URL-Filter

Controls which FQDNs the endpoint can reach or not



Bandwidth

Control maximum bandwidth and burst rate per endpoint/user



Calendar Profile

Controls active hours for endpoint access.



Timer

Control session, idle-timeout, active hours



QoS

QoS Profile is assigned per endpoint



AVC Profile

Application Visibility Profile is assigned per endpoint



mDNS Profile

Assigns mDNS profile to broker mDNS advertisement



Open DNS

Assigns Open DNS profile to intercept DNS packets for custom response



Service Template & Roles

Assigns multiple access characteristics: VLAN, ACL, QoS, Timer, etc.

Authorisation

Network Segmentation

Static VLAN Assignment

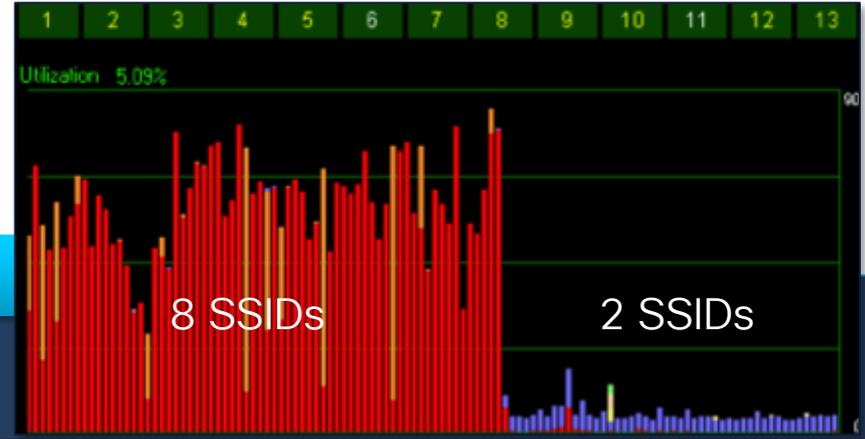
- VLAN based on SSID
- VLAN segregation based on security policy

Dynamic VLAN Assignment

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

TrustSec / Group Based 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

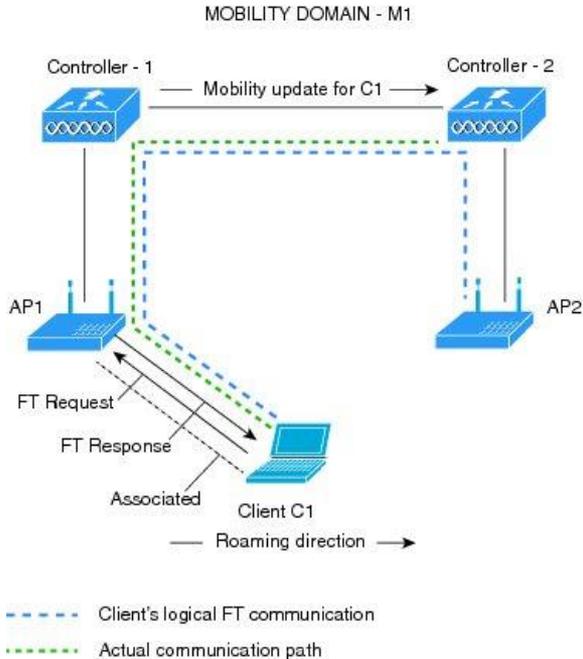
Secure Fast Roaming

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

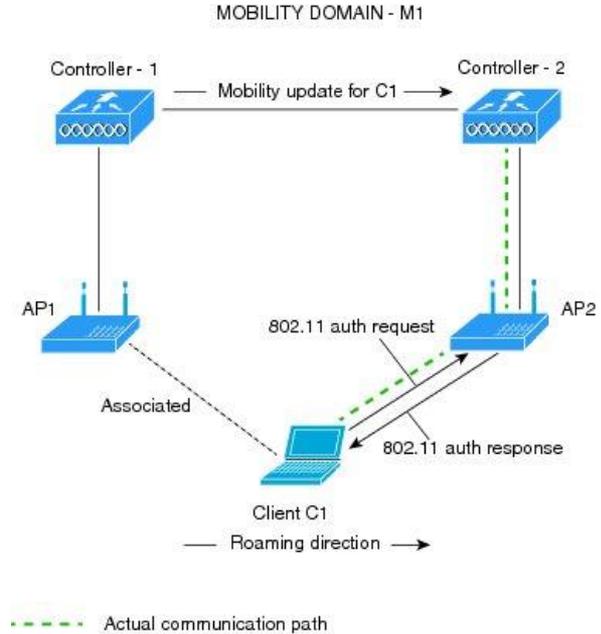


- Client channel scanning and AP selection
 - 802.11k Neighbor Lists based on CCX (Cisco Compatible Extensions)
 - 802.11v BSS Transition
- Re-authentication of client device and re-keying
 - 802.11r Fast BSS Transition based on CCKM (Cisco Centralised Key Management)

802.11r Fast Transition



Over the DS



Over the Air

802.11r Fast Transition



- Over the Air is recommended for best client interoperability

The screenshot shows the 'Add WLAN' configuration interface, specifically the 'Security' tab and 'Layer2' section. The 'Fast Transition' section is highlighted with a red box, showing the following settings:

- Status: Enabled
- Over the DS: Disabled
- Reassociation Timeout: 20

Other visible settings include:

- WPA + WPA2: Unselected
- WPA2 + WPA3: Selected
- WPA3: Unselected
- Static WEP: Unselected
- None: Unselected
- MAC Filtering: Unchecked
- Lobby Admin Access: Unchecked
- WPA Parameters: WPA Policy (Unchecked), WPA2 Policy (Checked), GTK Randomize (Unchecked), WPA3 Policy (Checked), Transition Disable (Unchecked)
- WPA2/WPA3 Encryption: AES(CCMP128) (Checked), CCMP256 (Unchecked), GCMP128 (Unchecked), GCMP256 (Unchecked)
- Protected Management Frame: PMF (Required)
- Auth Key Mgmt: 802.1x (Unchecked), PSK (Unchecked), CCKM (Unchecked), SAE (Unchecked), OWE (Unchecked), FT + 802.1x (Checked), 802.1x-SHA256 (Unchecked)
- MPSK Configuration: Unchecked



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](#)

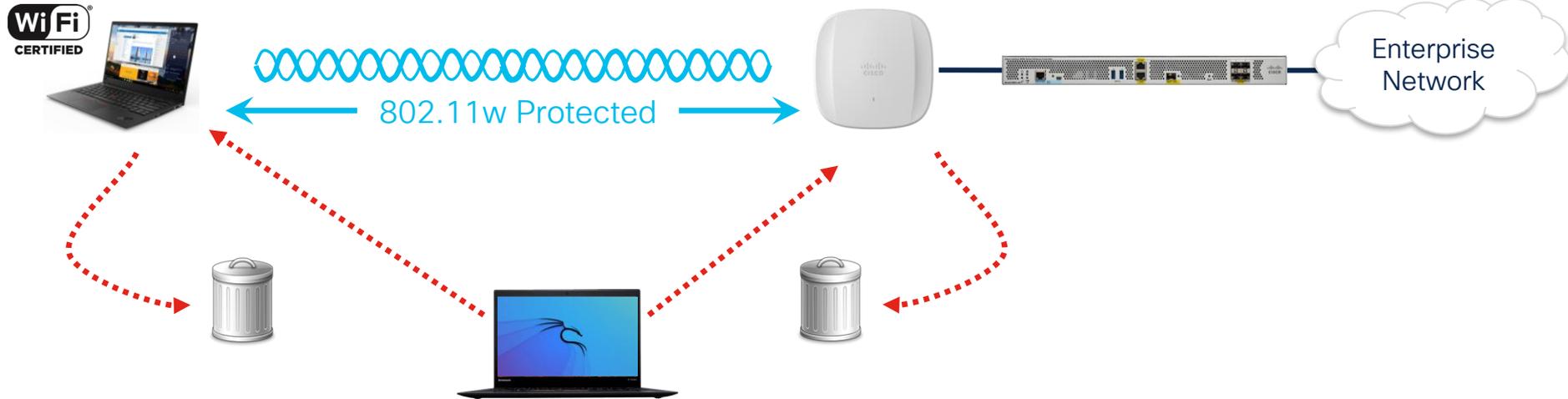
- This was an industry wide issue
 - Not specific to any one vendor
- WPA3 certification includes KRACK exploit testing
- The attacker positions a rogue AP clone to perform a MitM attack
 - This flaw causes all WPA2 encryption protocols to reuse the keystream when encrypting packets
- Rogue AP detection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

Kr00k Vulnerability

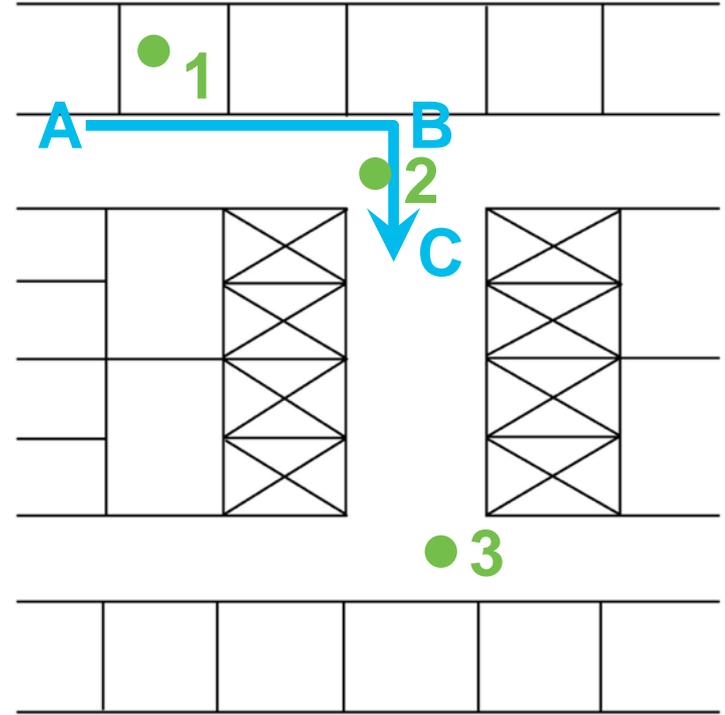
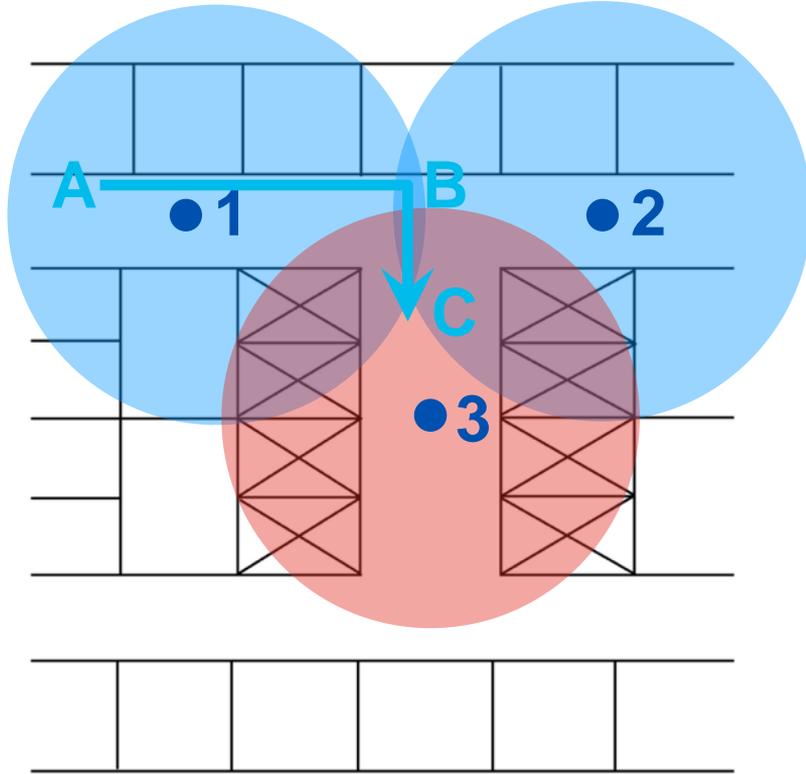


- On February 26th, 2020, researchers Štefan Svorencík and Robert Lipovsky [disclosed a vulnerability in the packet processing of certain Wi-Fi chipsets](#)
- This vulnerability could allow an unauthenticated, adjacent attacker to decrypt Wi-Fi frames without the knowledge of the PTK
- After an affected device handles a disassociation event, it could send a limited number of Wi-Fi frames encrypted with a static, weak PTK
- An attacker could exploit this vulnerability by triggering a disassociation and then acquiring these frames and decrypting them with the static PTK
- WIDS/WIPS can detect potential attack vectors

802.11w Protected Management Frames



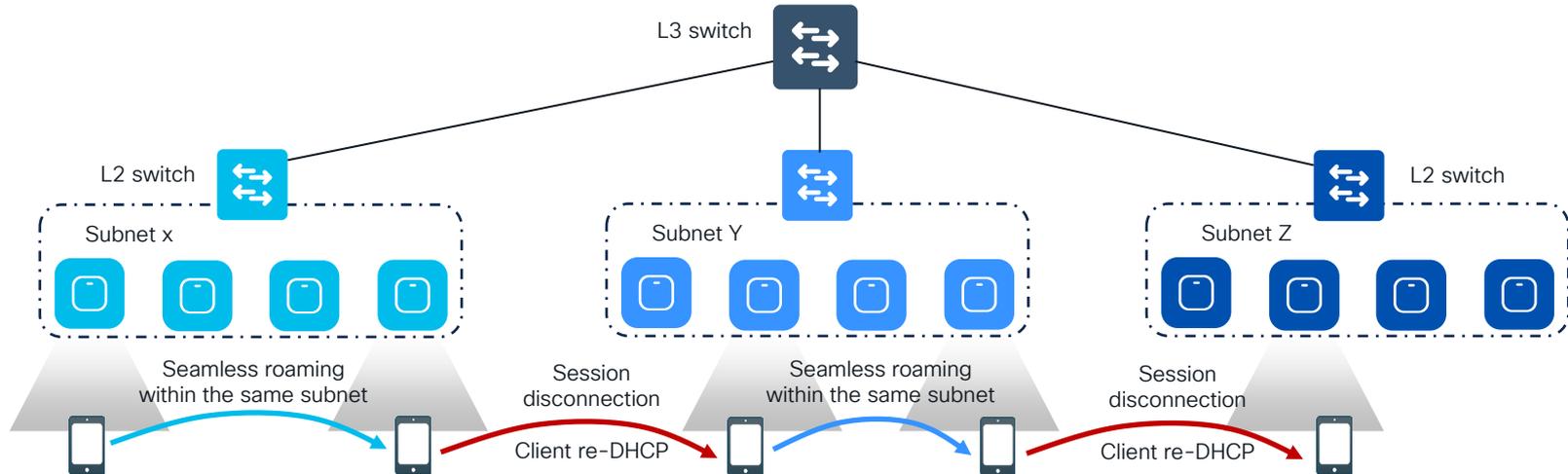
AP Placement and Roaming Optimization



Seamless Roaming at Scale

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

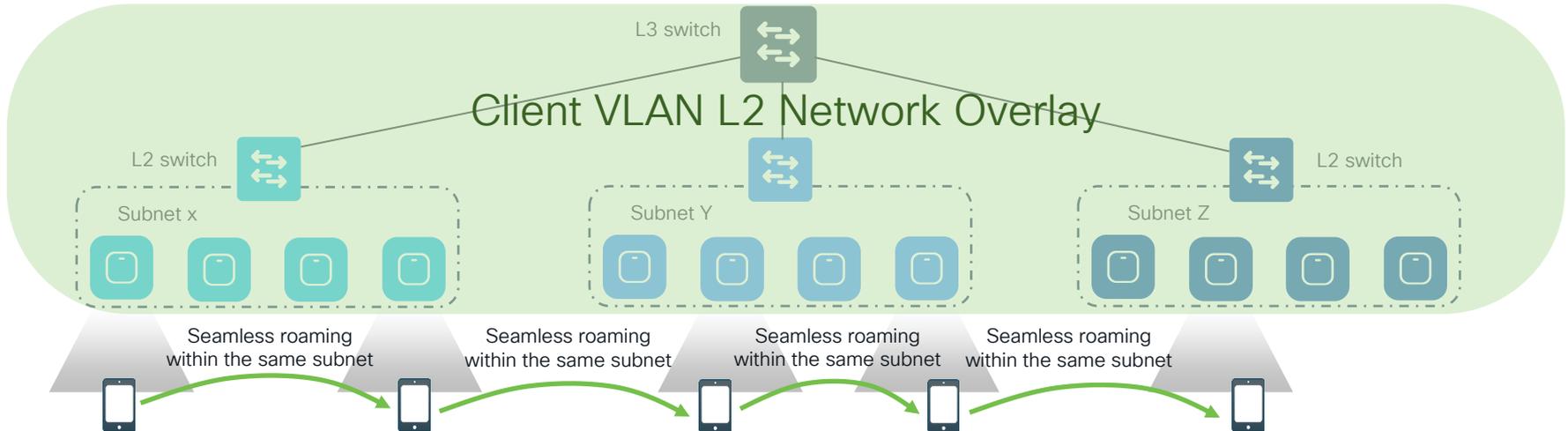
Large broadcast domains do not scale and is counter to networking best practice



Seamless Roaming at Scale

For L3 seamless roaming an extended VLAN network overlay is required

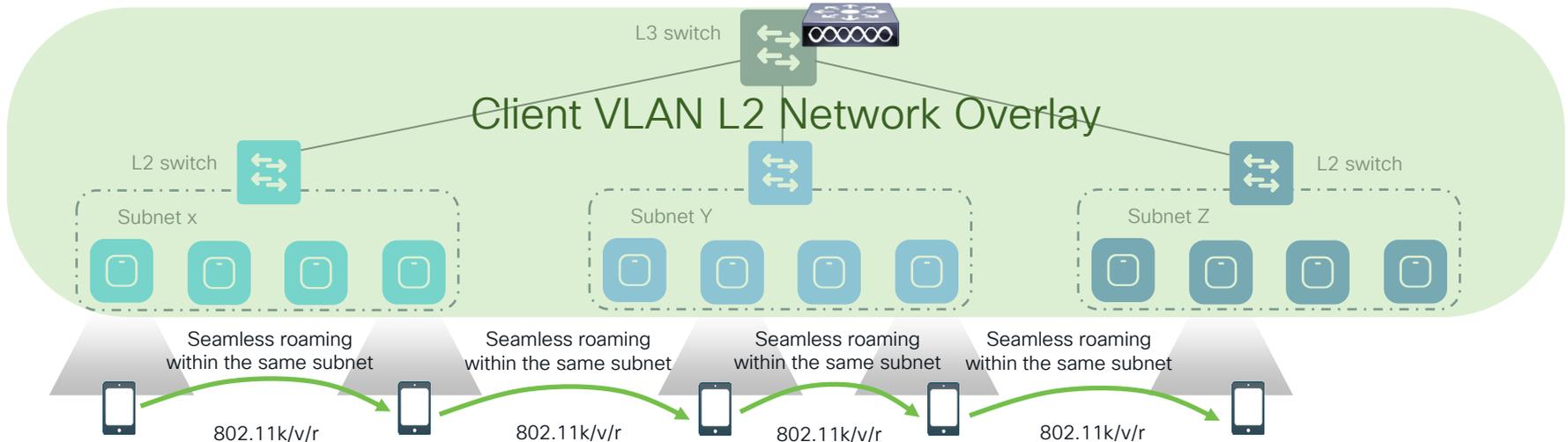
A data termination point is required to roam across L3 boundaries



Seamless Roaming at Scale

Edge Wireless Service
Data Plane (DP) Termination

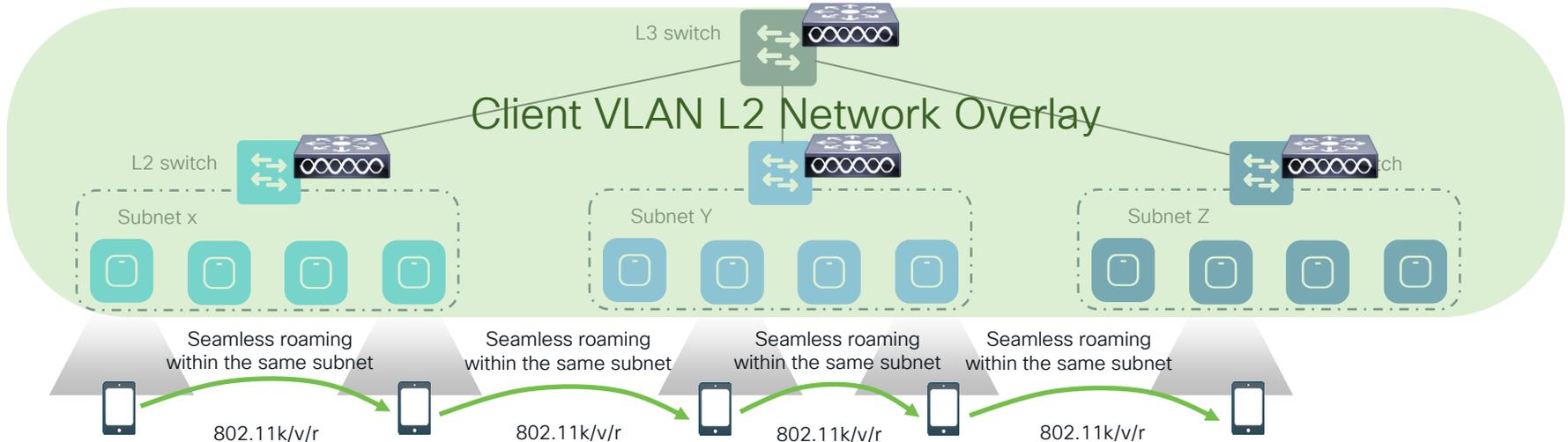
Can be deployed as centralized
(CAPWAP / EoGRE) or distributed
(fabric) architectures



Seamless Roaming at Scale

Edge Wireless Service
Data Plane (DP) Termination

Can be deployed as centralized
(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

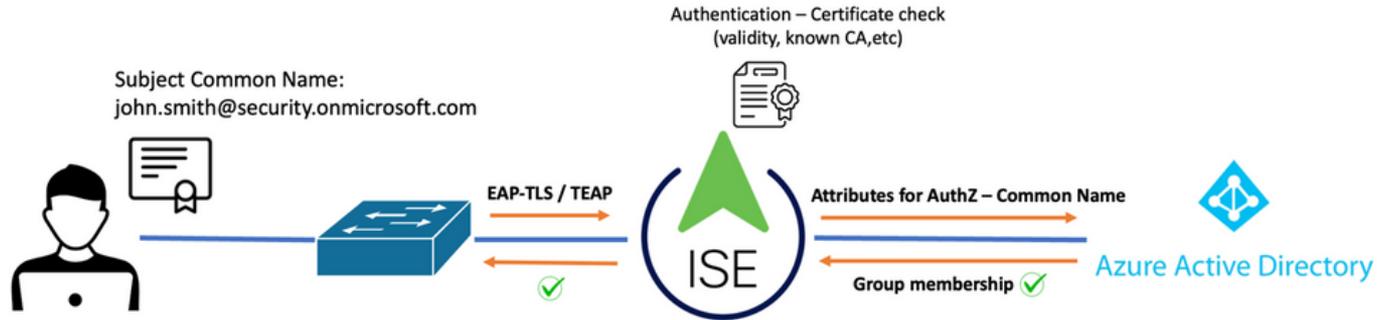
VPN, Application Access



SAMLv2, OpenID Connect



Cloud Identity with EAP-TLS



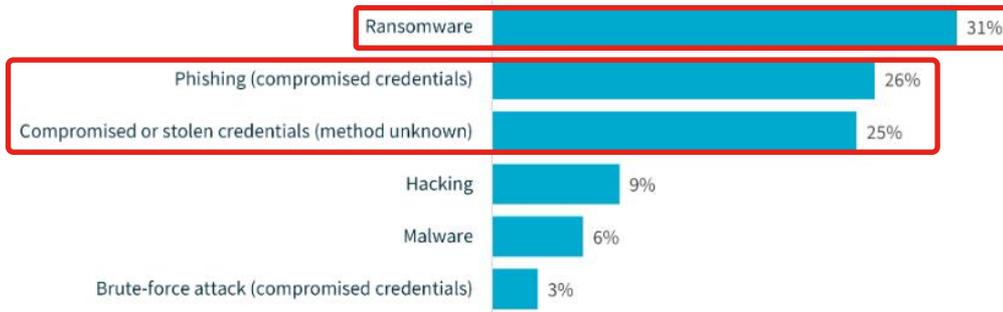
Multi-Factor Authentication



Zero Trust

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

Cyber incident breakdown

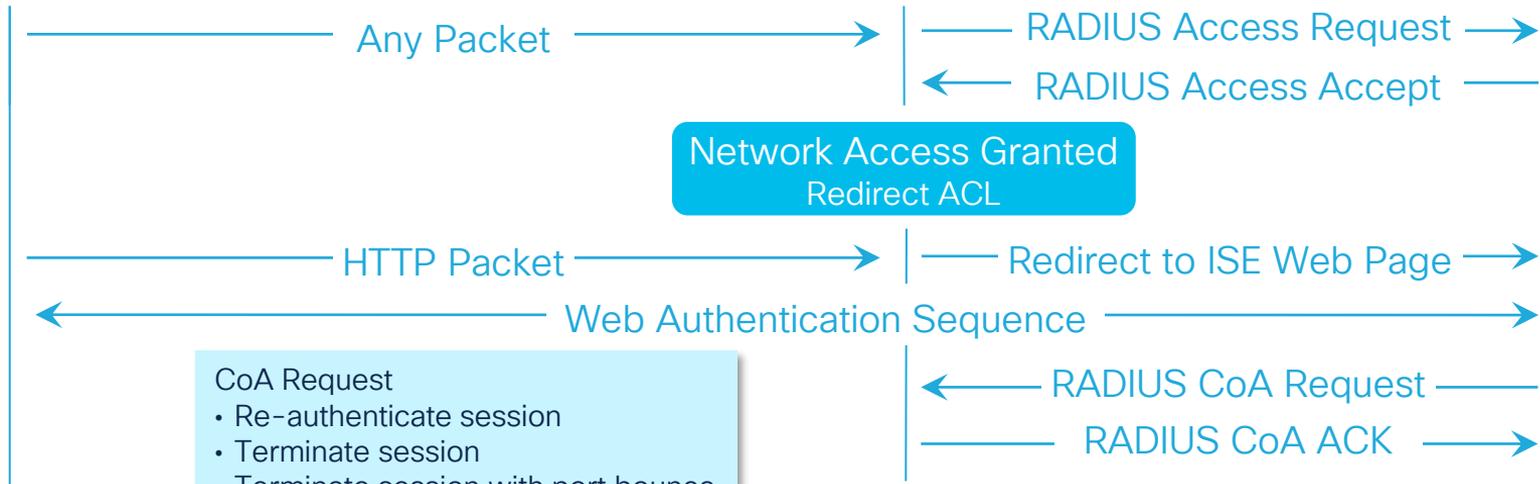


- Ransomware
 - East/West Traversal
 - Authorisation
 - Micro-segmentation
 - Rapid Threat Containment

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

Central Web Authentication

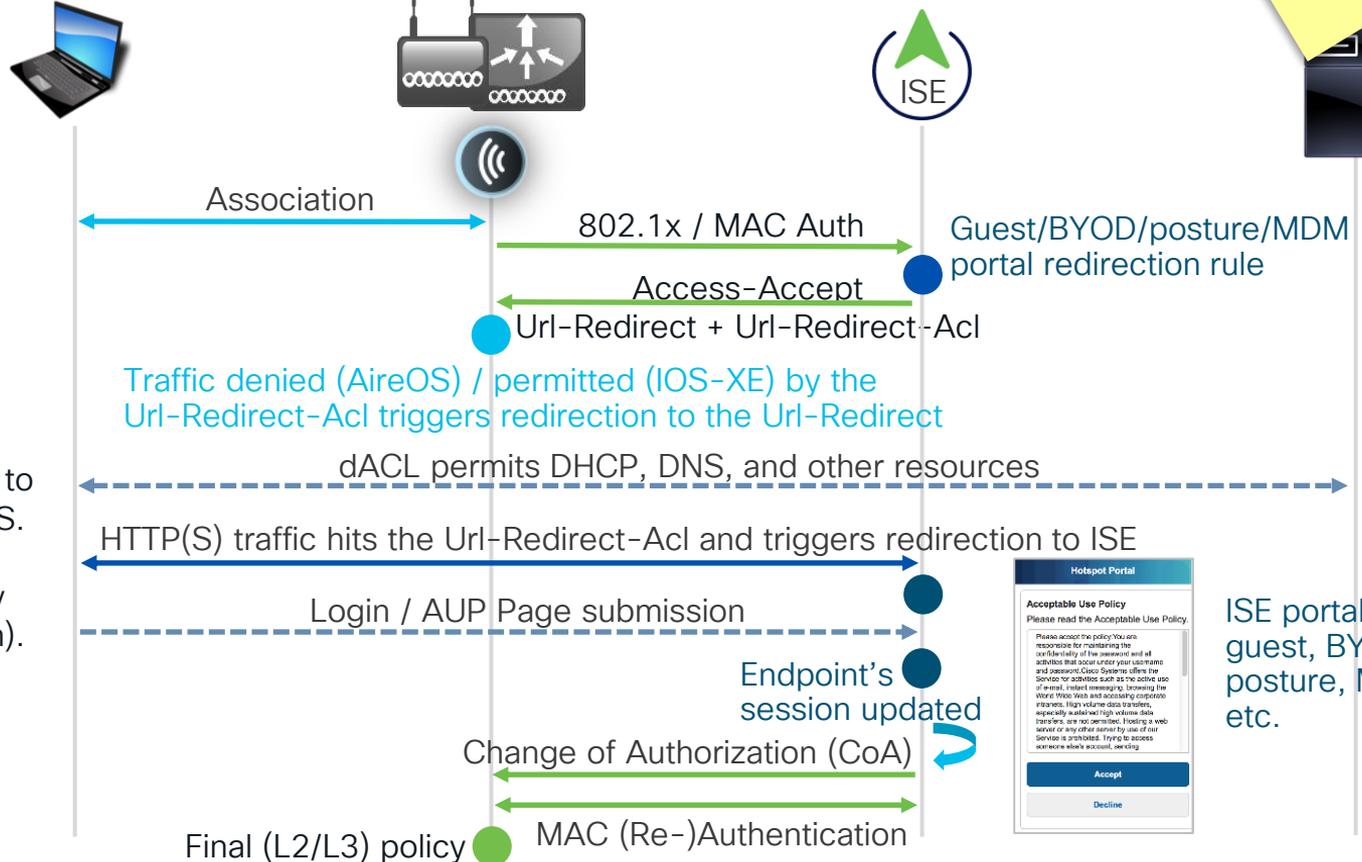
URL Redirect



CoA Request

- Re-authenticate session
- Terminate session
- Terminate session with port bounce
- Disable host port

Central Web Authentication



CENTRAL because the redirection URL, the pre-webauth ACL are **centrally** configured on ISE and dynamically communicated to the WLC (NAD*) via RADIUS. CWA is partially L2 (MAC Authentication) and partially L3 (redirect on IP resolution).

*Network Access Device

Self-Registration of BYOD Devices



CISCO My Devices Portal

Select an operation you would like to perform on your device.

Device status:
Device name:
Device ID:
Description:

Lost **Stolen**

Edit **Delete**

Close

2
Devices can be Blacklisted By the User.

1
New Devices Can be Added with a Description

CISCO My Devices Portal

Add Device

To add a new device, enter the device ID, which displays on your device as the MAC address. The device ID consists of 6 alphanumeric number pairs separated by colons such as AA:BB:CC:11:22:33.

Device name: *

Device ID: *

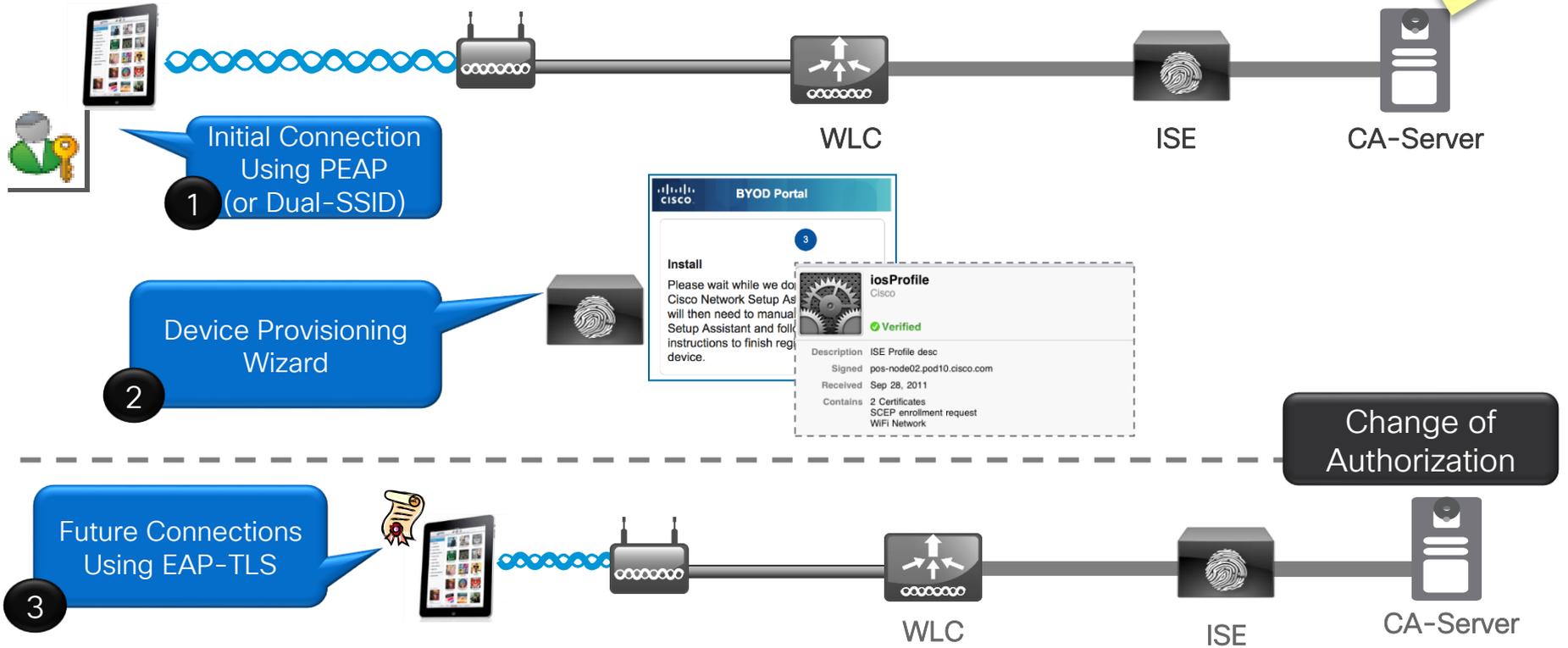
Description:

Submit **Cancel**

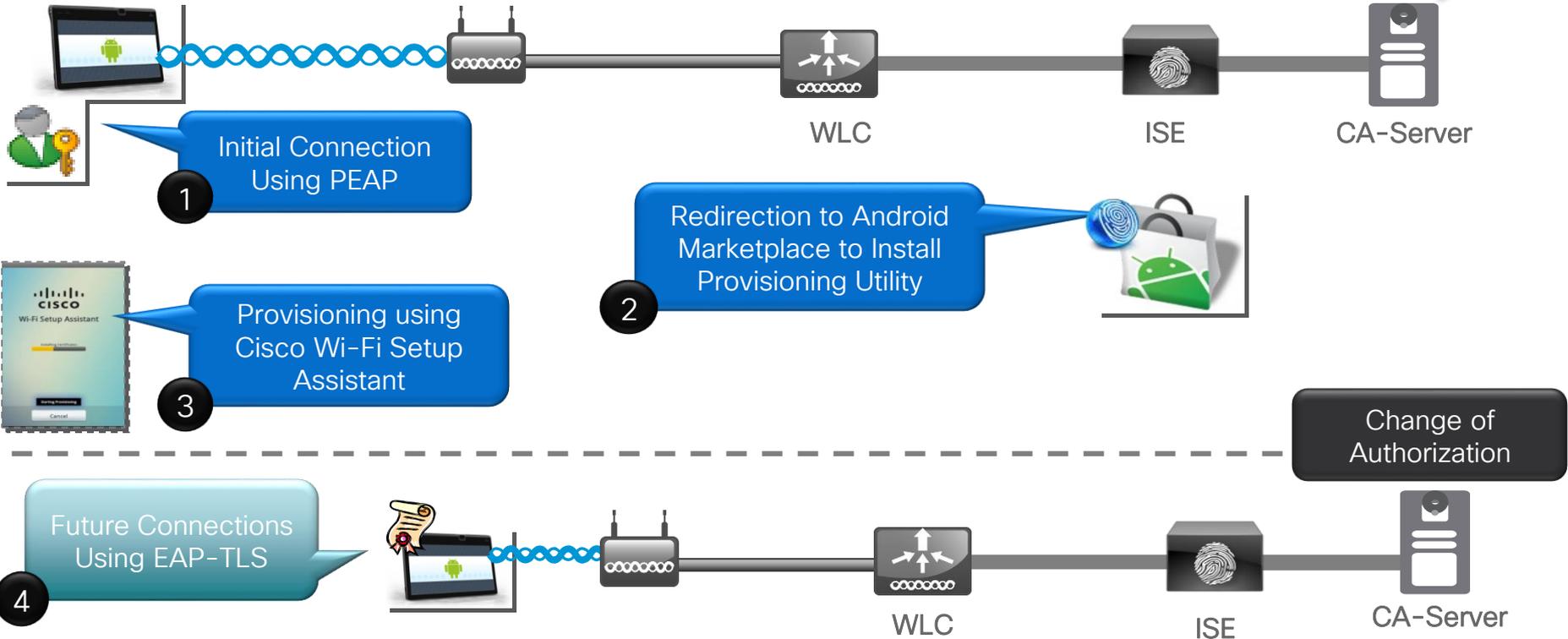
3
Devices Can be Self-Registered, Up to an Administrator Defined Limit

Client Provisioning

FYI



Android Device Provisioning



Client Provisioning Policy

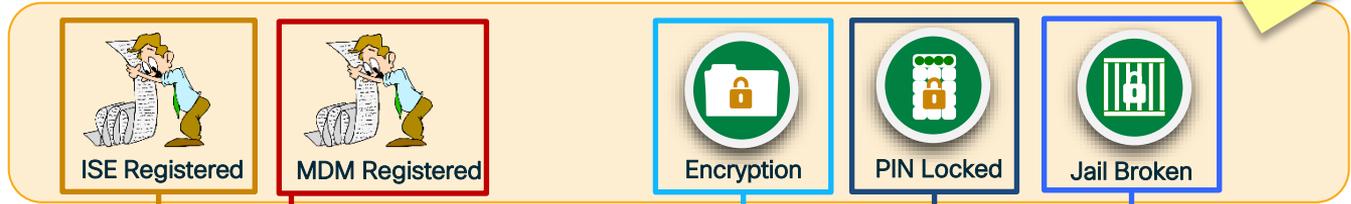


Client Provisioning Policy

Define the Client Provisioning Policy to determine what users will receive upon login and user session initiation:
For Agent Configuration: version of agent, agent profile, agent compliance module, and/or agent customization package.
For Native Supplicant Configuration: wizard profile and/or wizard.

Rule Name	Identity Groups	Operating Systems	Other Conditions	Results
<input checked="" type="checkbox"/> IOS	If Any and	Mac iOS All and	AD1:ExternalGroups EQUALS cts.I... and	WiFi_Profile
<input checked="" type="checkbox"/> Android	If Any and	Android and	AD1:ExternalGroups EQUALS cts.I... and	WiFi_Profile
<input checked="" type="checkbox"/> WinThings	If Any and	Windows... and	AD1:ExternalGroups EQUALS cts.I... and	WinSPWizard 1.0.0.14 And WiFi_Profile
<input checked="" type="checkbox"/> MAC-OSX	If Any and	Mac OSX and	AD1:ExternalGroups EQUALS cts.I... and	MacOsXSPWizard 1.0.0.6 And WiFi_Profile

MDM Integration



MobileDevice_Compliant	if RegisteredDevices AND (MDM:DiskEncryptionStatus EQUALS On AND MDM:PinLockStatus EQUALS On AND MDM:JailBrokenStatus EQUALS Unbroken)	then Employee_MobileDevice
MobileDevice_Unregistered	if RegisteredDevices AND MDM:DeviceRegisterStatus EQUALS UnRegistered	then MDM_Registration
MobileDevice_NonCompliant	if RegisteredDevices AND (MDM:DiskEncryptionStatus EQUALS Off OR MDM:PinLockStatus EQUALS Off OR MDM:JailBrokenStatus EQUALS Broken)	then MDM_NonCompliance



Captive Portal Detection

- Native operating system support to detect captive portals
- User is aware of captive portal even when not using browser
- Simplifies guest access adoption
- Avoids the need to redirect HTTPS traffic



Windows

- <http://www.msftncsi.com/ncsi.txt>



Google Devices

- http://www.gstatic.com/generate_204

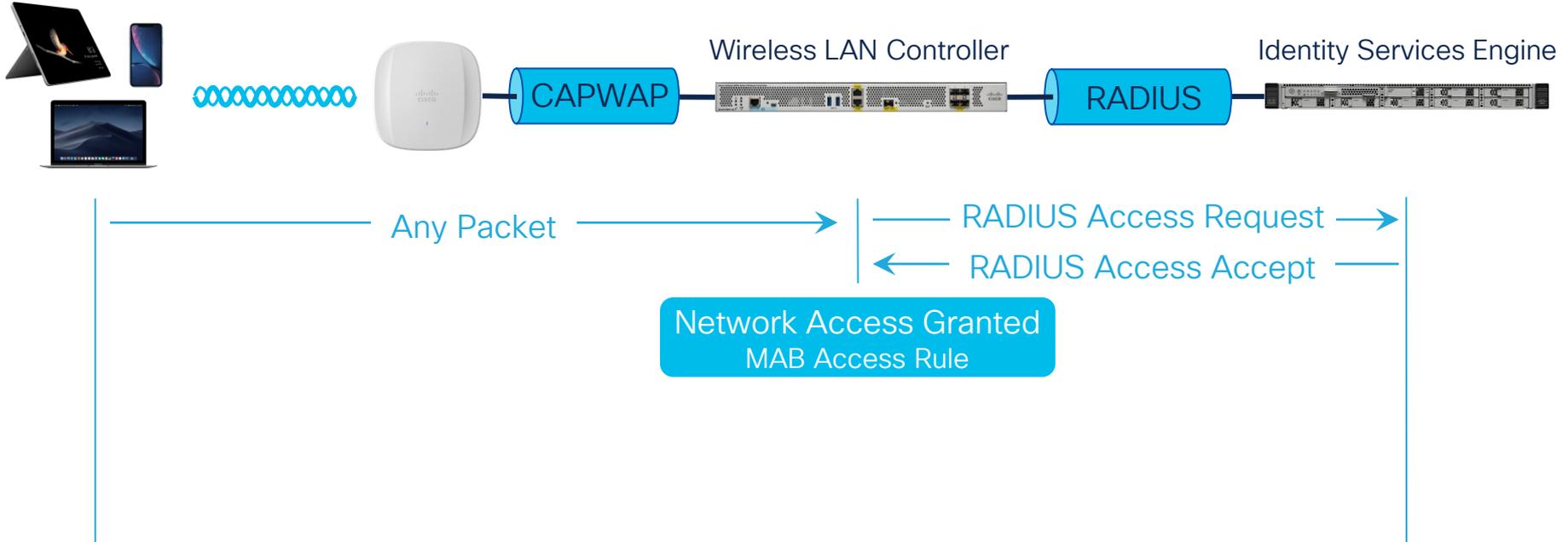


Apple Devices

- <http://captive.apple.com/hotspot-detect.html>

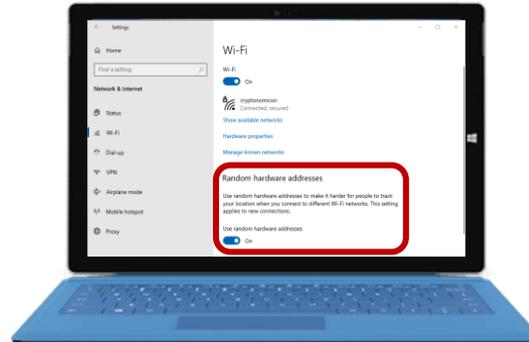
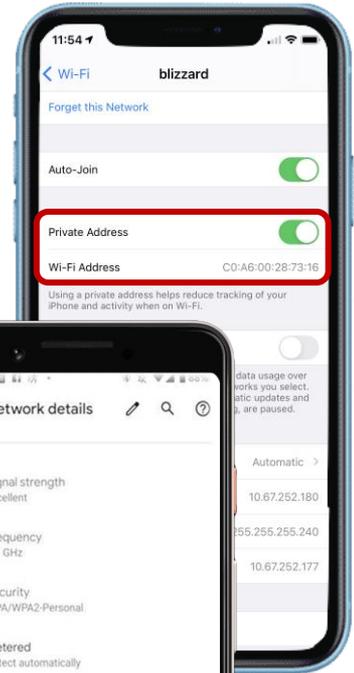
Central Web Authentication

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



Detailed implementation



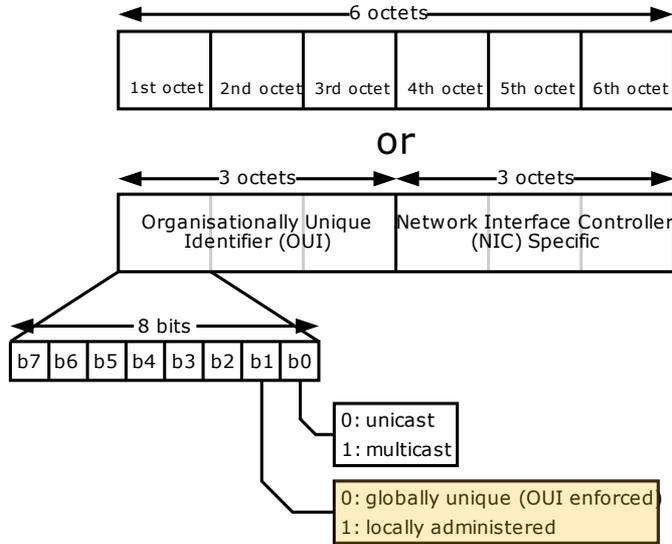
	Windows 10+	Android 10+	iOS 14+, iPadOS 14+, watchOS 7+
Randomization enabled by default	No	Yes	Yes
Same random MAC used for subsequent connection	Yes	Yes	Yes
Randomization saved between device reboot	Yes	Yes	Yes
Random MAC saved when Wi-Fi profile recreated	No	Yes	Yes
Randomization per day and/or per association	Optional	Optional (Android 11 Developer Mode)	No
Randomization enabled upon upgrade for existing Wi-Fi profile	No	No	Yes
Can be enabled/disabled globally	Yes	No	No
API to control randomization exists	Unknown	Yes (Android 11+)	Yes
Randomization saved between factory reset	No	No	Unknown

Random MAC Implications



 <p>Profiling</p>	 <p>BYOD</p>	 <p>Whitelisting</p>	 <p>MDM Flow</p>	 <p>Guest</p>
 <p>Location lookup</p>	 <p>User Defined Network</p>	 <p>Endpoint Analytics</p>	 <p>Forensics</p>	 <p>Quarantine</p>

Detecting Random MAC Addresses



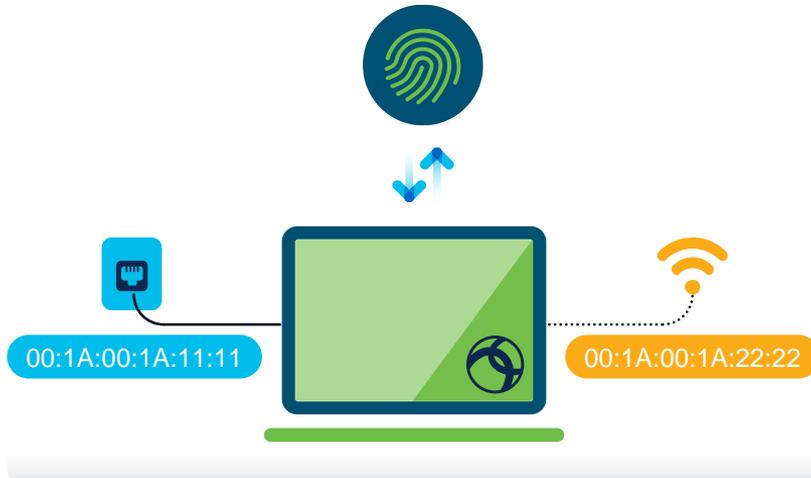
32-28-6D-51-13-AF
56-EF-68-F6-0D-30
0A-13-A8-8E-B5-EF
AE-83-37-55-A7-22

By Inductiveload, modified/corrected by Kju - SVG drawing based on PNG uploaded by User:Vtraveller. This can be found on Wikipedia here., CC BY-SA 2.5, <https://commons.wikimedia.org/w/index.php?curid=1852032>

Unique Device Identifier

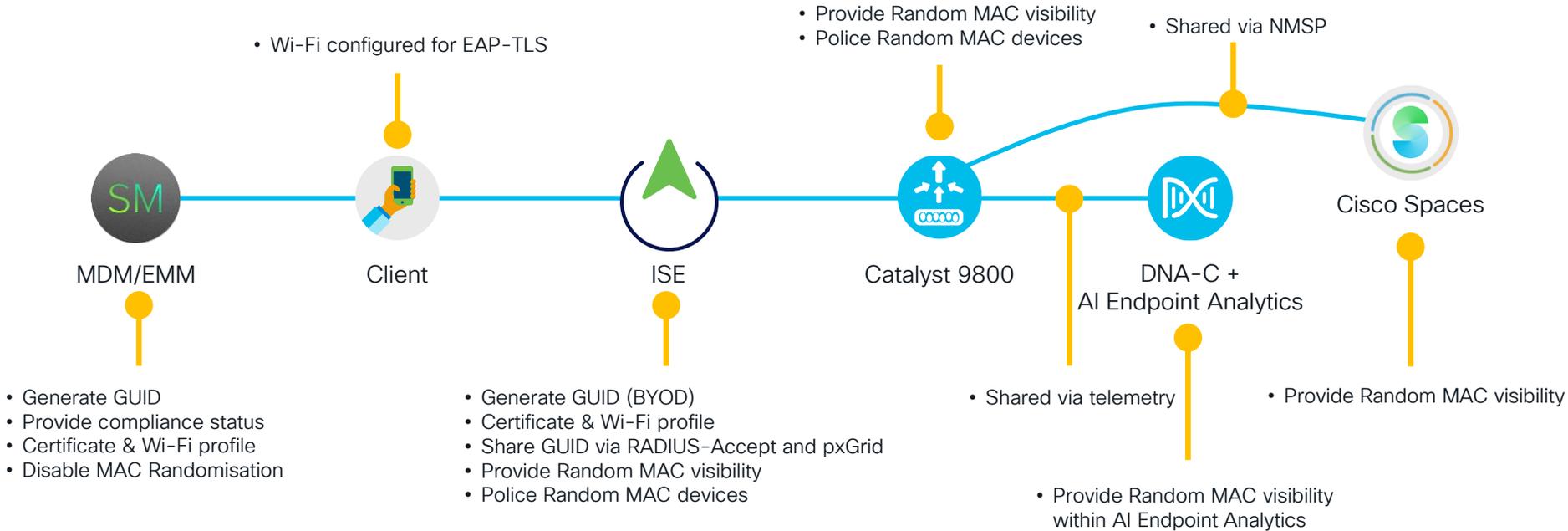


UDID	MAC Address(s)	Compliance
01669b65...05ee93	00:1a:00:1a:11:11 00:1a:00:1a:22:22	✓

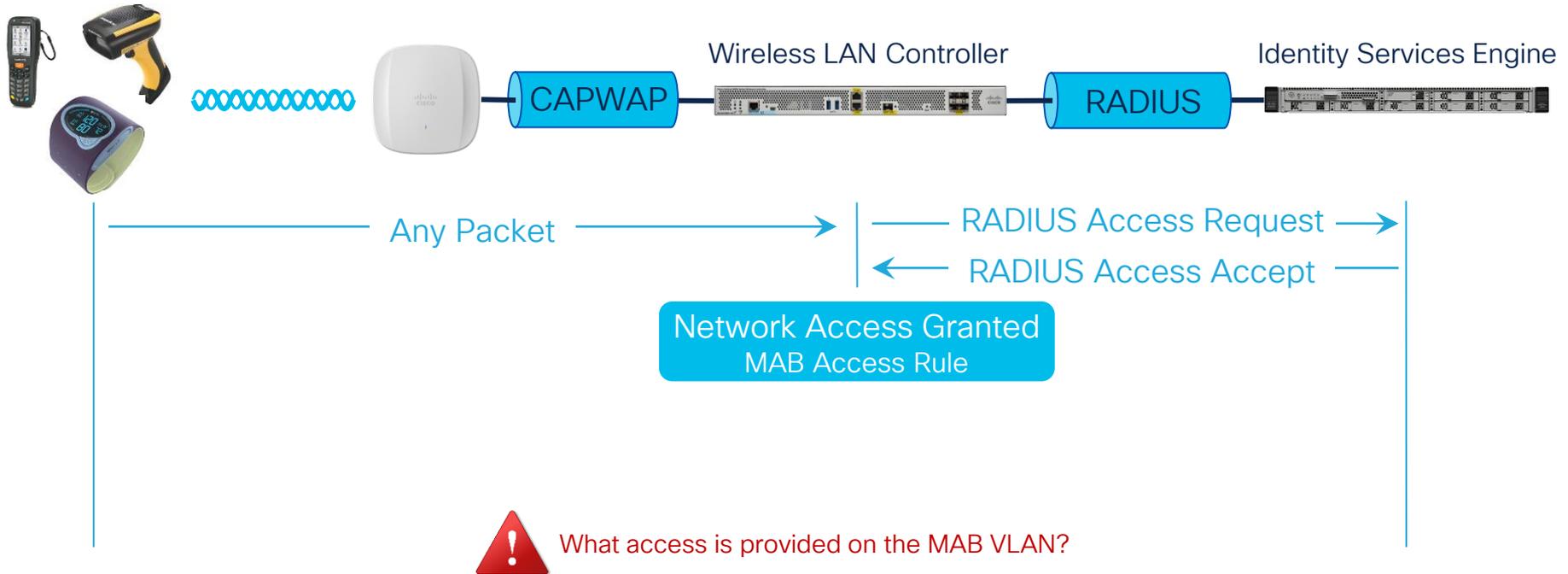


- In open seating environments with docking stations for PCs and Ethernet dongles for Apple MacBooks, lead to a different challenge:
- The same MAC address will be used by different users.
- ISE can perform authorization for managed end-points leveraging the laptop UDID (Unique Device Identifier) instead of the MAC address.
- Requirements
ISE 2.6, AnyConnect 4.7

Globally Unique Identifier



MAC Authentication Bypass



Wi-Fi Certified Easy Connect

WPA3



Device Provisioning Protocol (DPP)

- 3 Phases
 - Bootstrapping
 - Obtains the public key of new device
 - Authentication and Provisioning
 - Public key is used to create a secure tunnel for credential exchange
 - Network Access
 - PMK derived
 - Four-Way Handshake used as normal
 - Supports Protected Management Frames



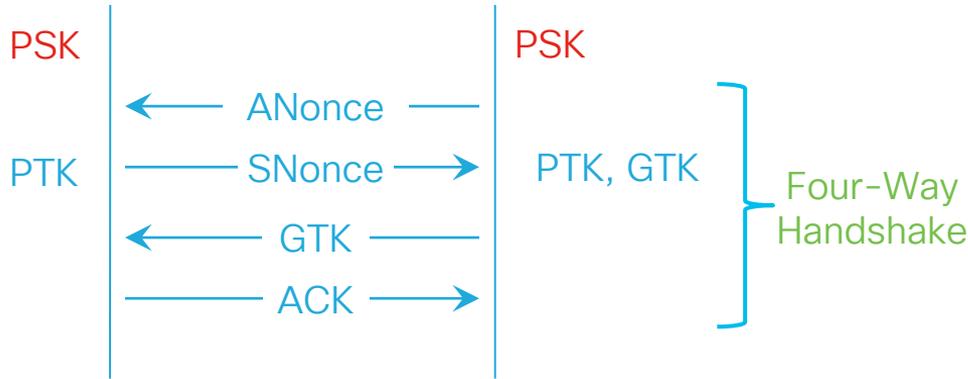
WPA Personal

Pre-Shared Key



WPA Personal

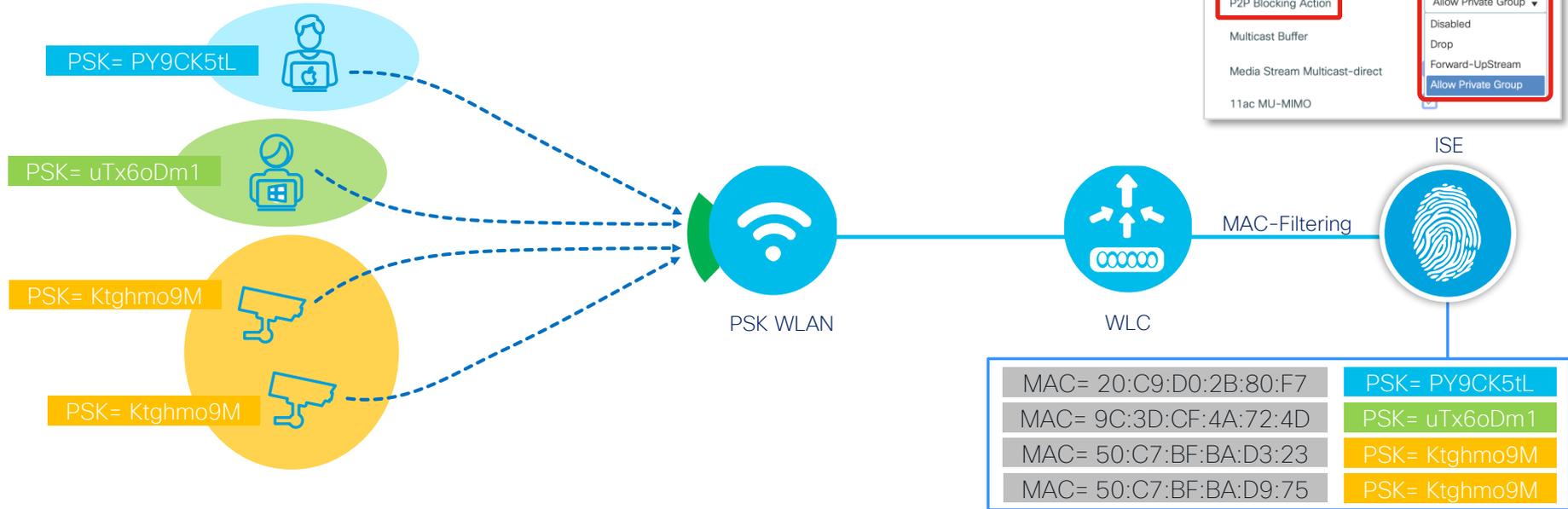
Pre-Shared Key



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

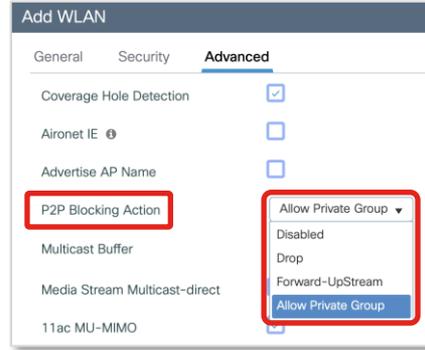
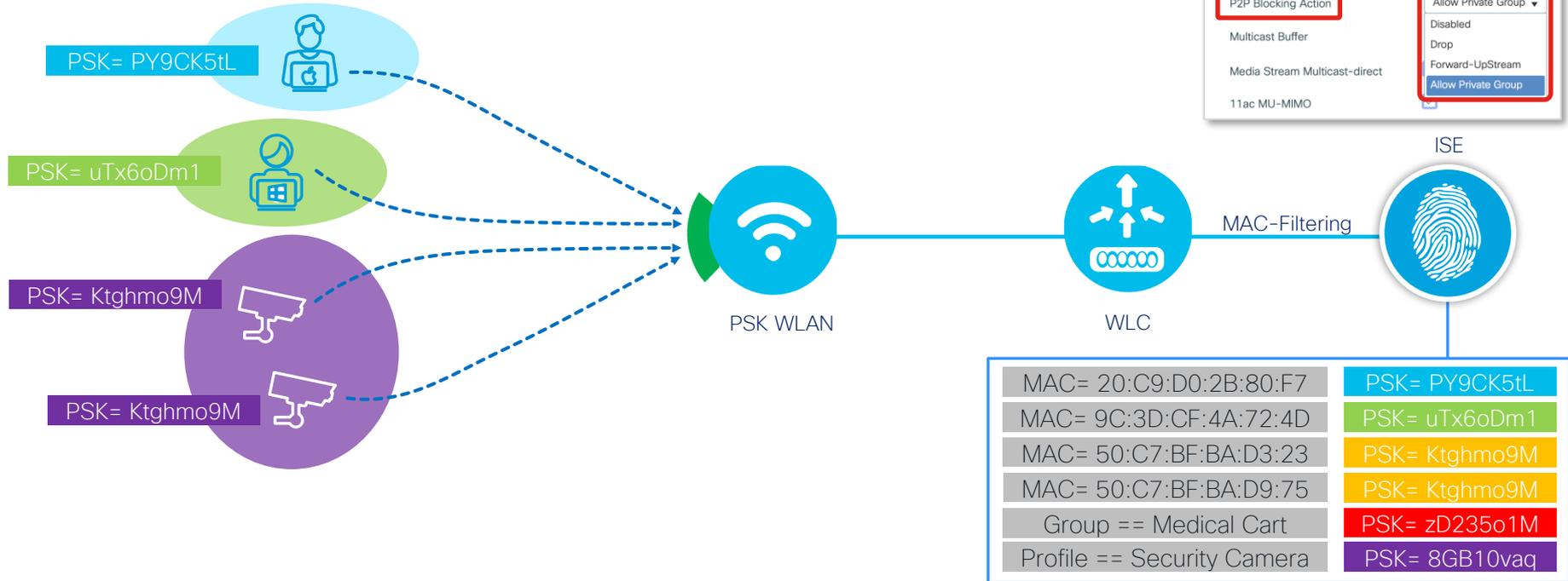
- Offline Attacks
 - Dictionary
 - Rainbow Table
- Strong Passwords Matter

Identity PSK



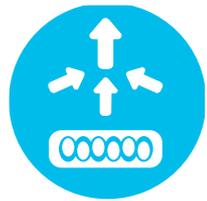
<https://www.cisco.com/c/en/us/support/docs/wireless/catalyst-9800-series-wireless-controllers/216130-configure-catalyst-9800-wlc-ipsk-with-ci.html>
https://documentation.meraki.com/MR/Encryption_and_Authentication/IPSK_with_RADIUS_Authentication

Identity PSK

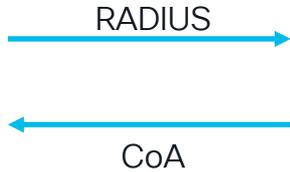


<https://www.cisco.com/c/en/us/support/docs/wireless/catalyst-9800-series-wireless-controllers/216130-configure-catalyst-9800-wlc-ipsk-with-ci.html>
https://documentation.meraki.com/MR/Encryption_and_Authentication/IPSK_with_RADIUS_Authentication

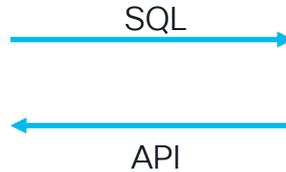
iPSK Manager



WLC / AP



ISE



iPSK Manager

- Linux
- Apache
- MySQL
- PHP



Administration

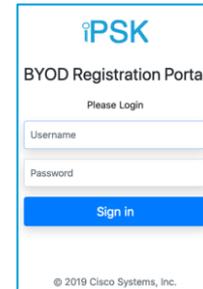


Admin

iPSK Lifecycle Management



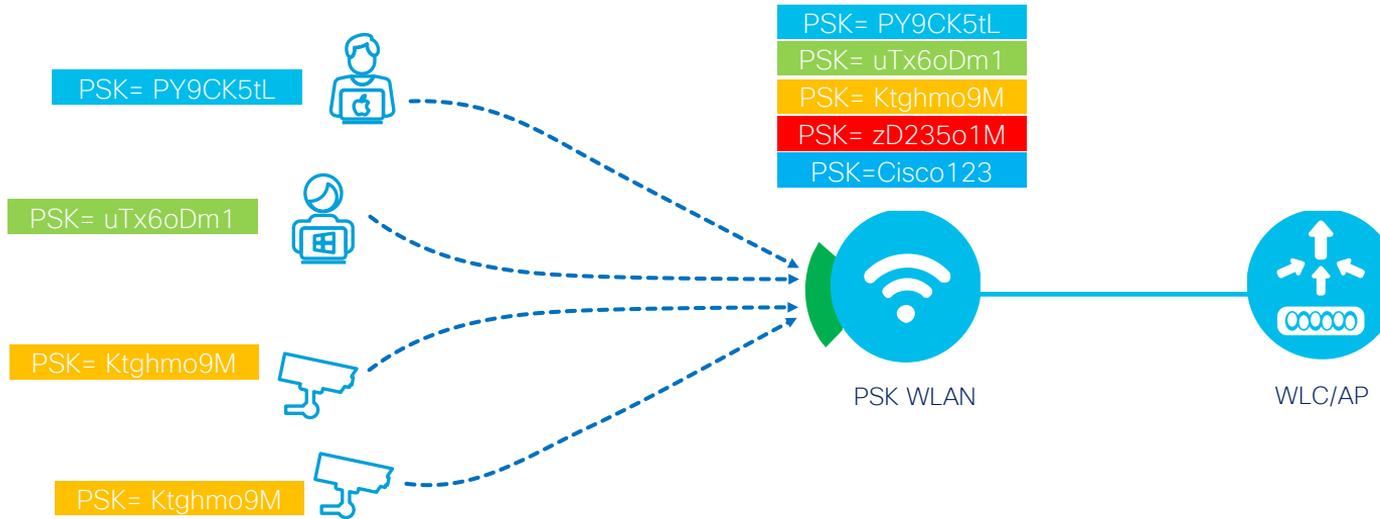
End Users



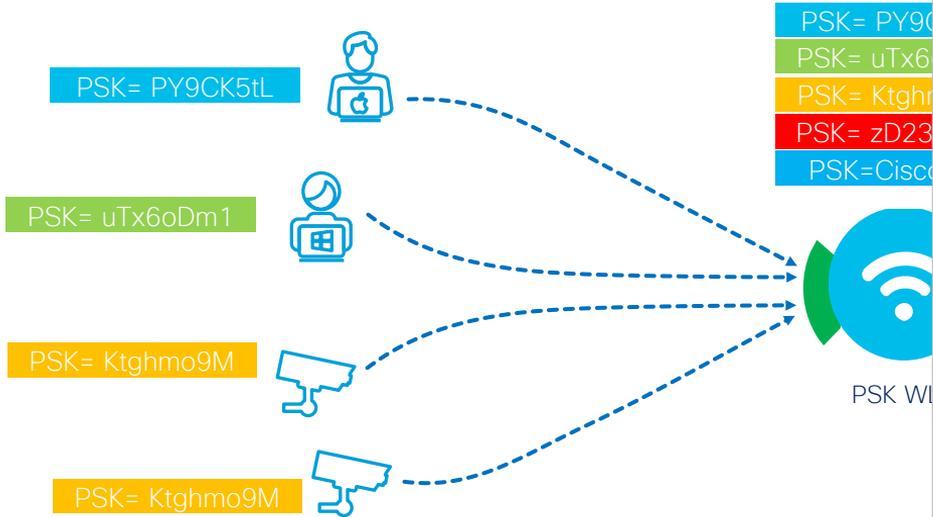
<http://cs.co/iPSK-Manager>

CISCO *Live!*

Multi Pre-Shared Key



Multi Pre-Shared Key



Edit WLAN

General **Security** Advanced Add To Policy Tags

Layer2 Layer3 AAA

WPA + WPA2 WPA2 + WPA3 WPA3 Static WEP

MAC Filtering Authorization List* mpsk ⓘ

Lobby Admin Access

WPA Parameters

WPA Policy	<input type="checkbox"/>	WPA2 Policy	<input checked="" type="checkbox"/>
GTK Randomize	<input type="checkbox"/>	OSEN Policy	<input type="checkbox"/>

WPA2 Encryption

AES(CCMP128)	<input checked="" type="checkbox"/>	CCMP256	<input type="checkbox"/>
GCMP128	<input type="checkbox"/>	GCMP256	<input type="checkbox"/>

Protected Management Frame

PMF Disabled

Fast Transition

Status Disabled

Over the DS

Reassociation Timeout * 20

Auth Key Mgmt

802.1x	<input type="checkbox"/>	PSK	<input checked="" type="checkbox"/>
Easy-PSK	<input type="checkbox"/>	CKKM ⚠	<input type="checkbox"/>
FT + 802.1x	<input type="checkbox"/>	FT + PSK	<input type="checkbox"/>
802.1x-SHA256	<input type="checkbox"/>	PSK-SHA256	<input type="checkbox"/>

PSK Format ASCII

PSK Type Unencrypted

Pre-Shared Key*

MPSK Configuration

Enable MPSK

+ Add - Delete

Priority Key Format Password Type

Priority * Priority(0-4)

Key Format ASCII

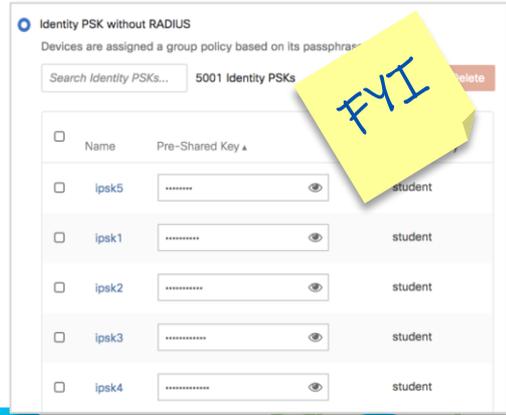
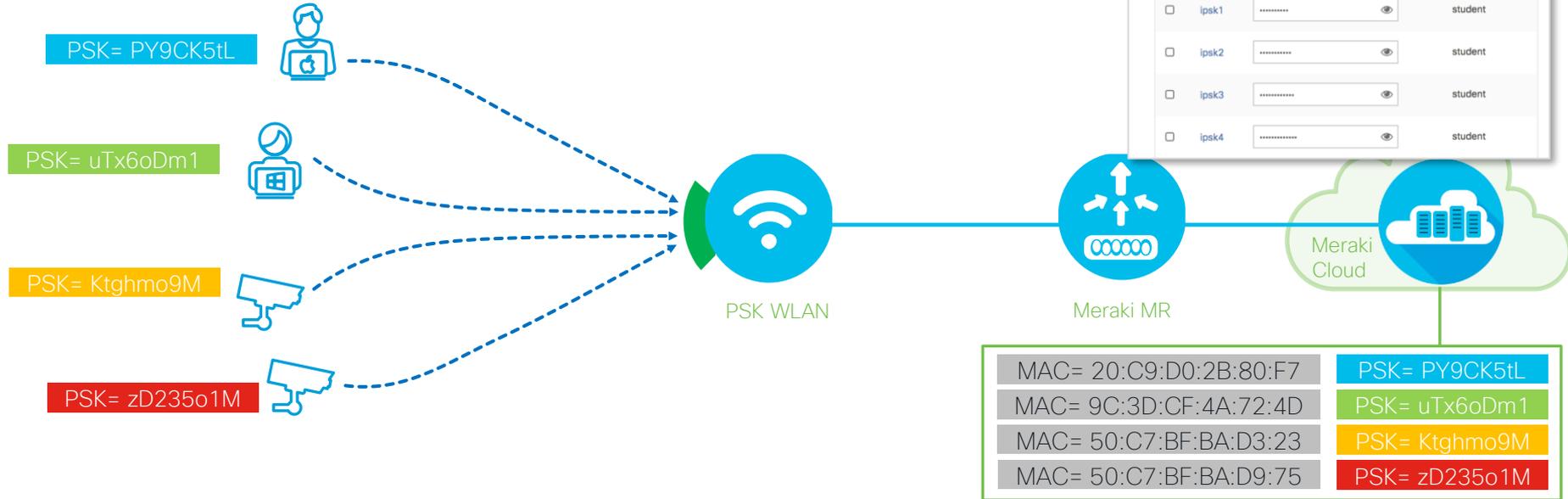
Password Type Unencrypted

Pre-Shared Key*

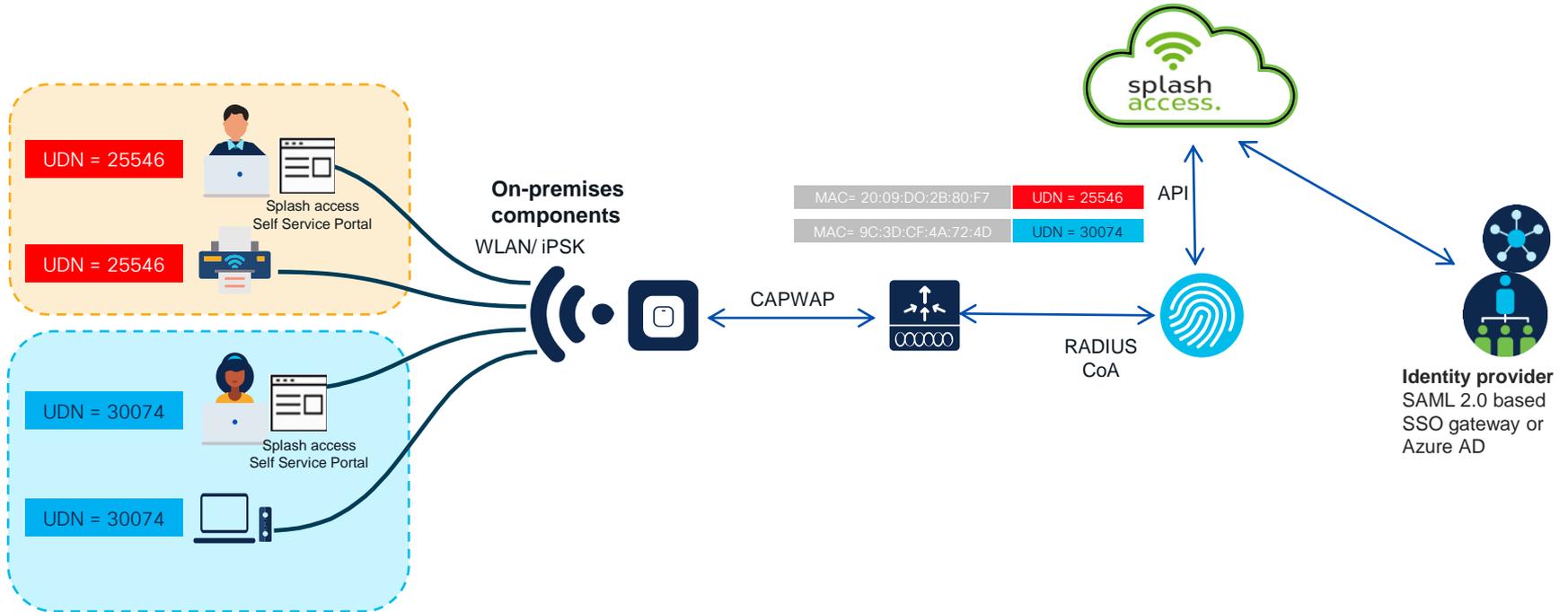
Cancel Apply

FYI

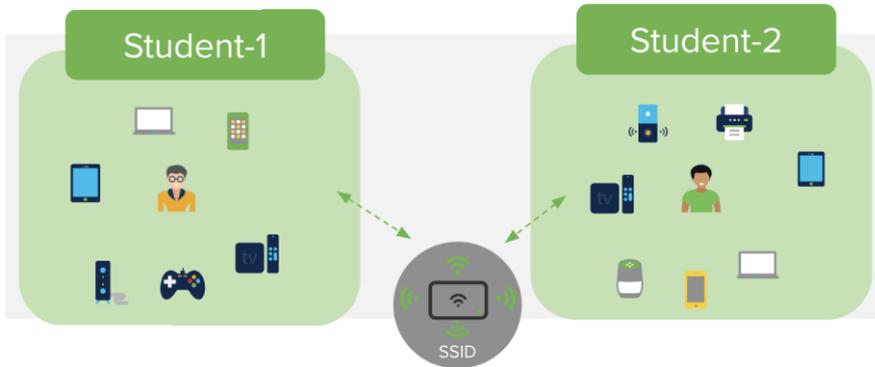
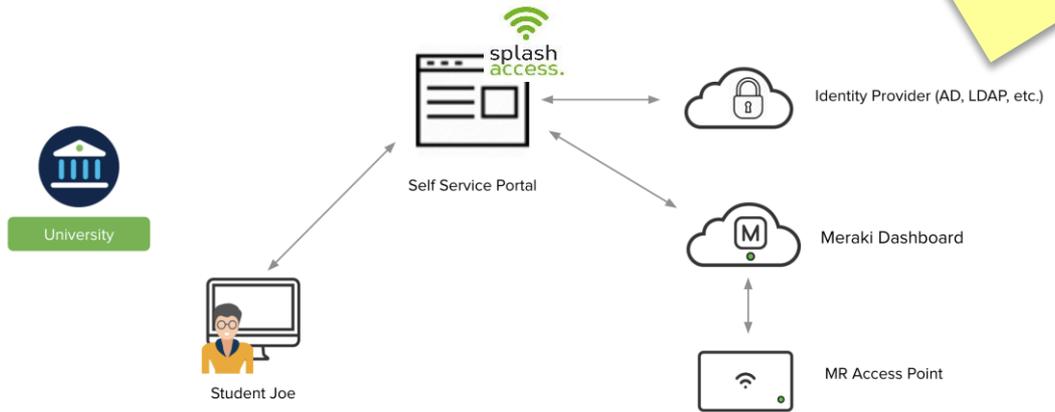
Identity PSK without RADIUS



User Defined Network



Wi-Fi Personal Network





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

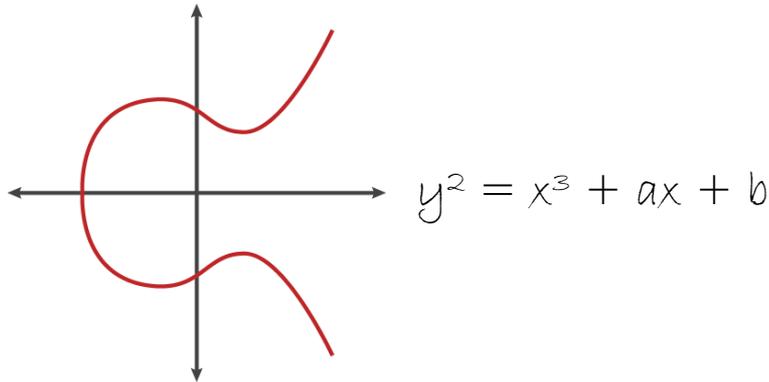
Dragonblood



- Backwards Compatibility Attack
 - Clients can be tricked into connecting to a Rogue WPA2 Personal only network
 - The attacker uses the partial WPA2 handshake for offline attacks
 - Certain devices, even when connected to WPA3 Personal only networks, could be tricked into using WPA2
- Denial of Services Attacks
 - APs should implement anti-exhaustion mechanisms
 - APs should implement detection mechanism and blacklist misbehaving clients

Dragonblood

- Timing-Based Side-Channel Attacks
 - The time it takes an AP to respond to commit frames may leak information about the password



Edit WLAN

General Security Advanced Add To Policy Tags

Layer2 Layer3 AAA

WPA + WPA2 WPA2 + WPA3 WPA3 Static WEP None

MAC Filtering Authorization List* ⓘ

Lobby Admin Access

WPA Parameters

WPA Policy	<input type="checkbox"/>	WPA2 Policy	<input type="checkbox"/>
GTK Randomize	<input type="checkbox"/>	WPA3 Policy	<input checked="" type="checkbox"/>
Transition Disable	<input checked="" type="checkbox"/>		

Fast Transition

Status ▾

Over the DS

Reassociation Timeout*

WPA2/WPA3 Encryption

AES(CCMP128)	<input checked="" type="checkbox"/>	CCMP256	<input type="checkbox"/>
GCMP128	<input type="checkbox"/>	GCMP256	<input type="checkbox"/>

Protected Management Frame

PMF ▾

Association Comeback Timer*

SA Query Time*

Auth Key Mgmt

SAE	<input checked="" type="checkbox"/>	FT + SAE	<input type="checkbox"/>
OWE	<input type="checkbox"/>	FT + 802.1x	<input type="checkbox"/>
802.1x-SHA256	<input type="checkbox"/>		

Anti Clogging Threshold*

Max Retries*

Retransmit Timeout*

PSK Format

PSK Type

Pre-Shared Key*

Hash to Element Only

Hunting and Pecking Only

Hash to Element O...



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

Access and Identity

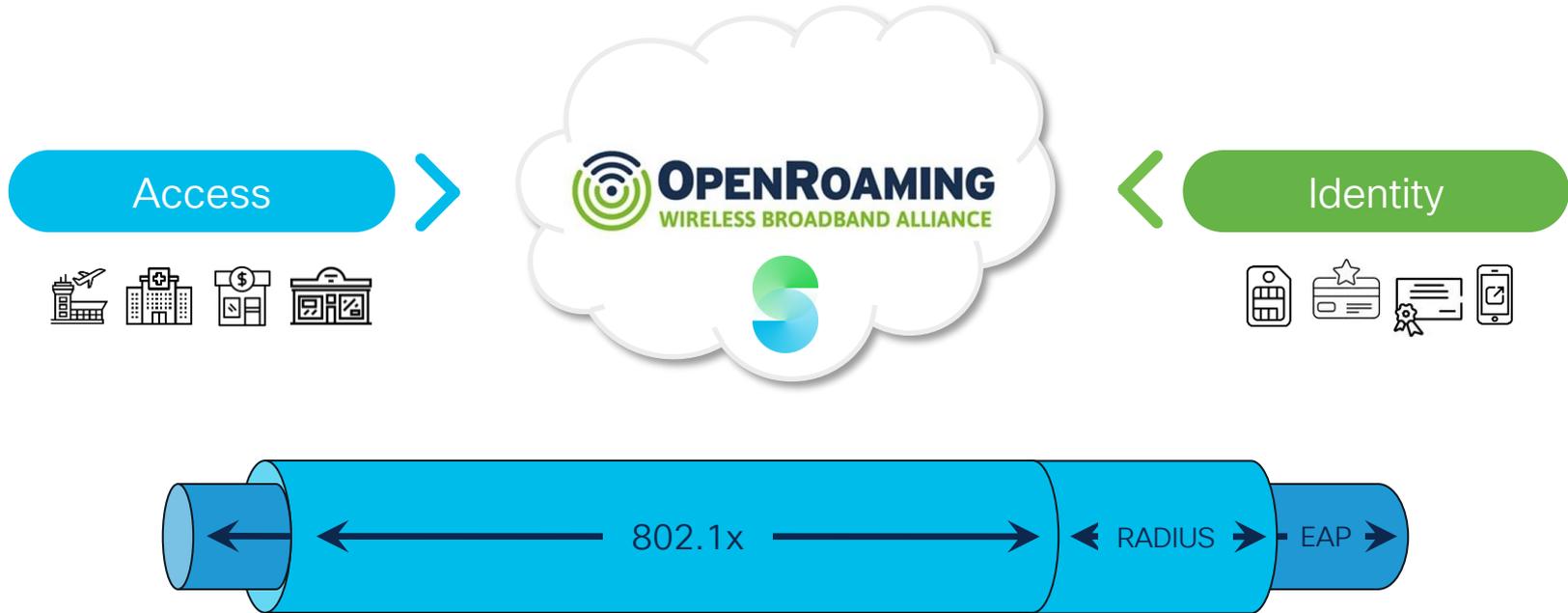
Decoupling Access and Identity

Access

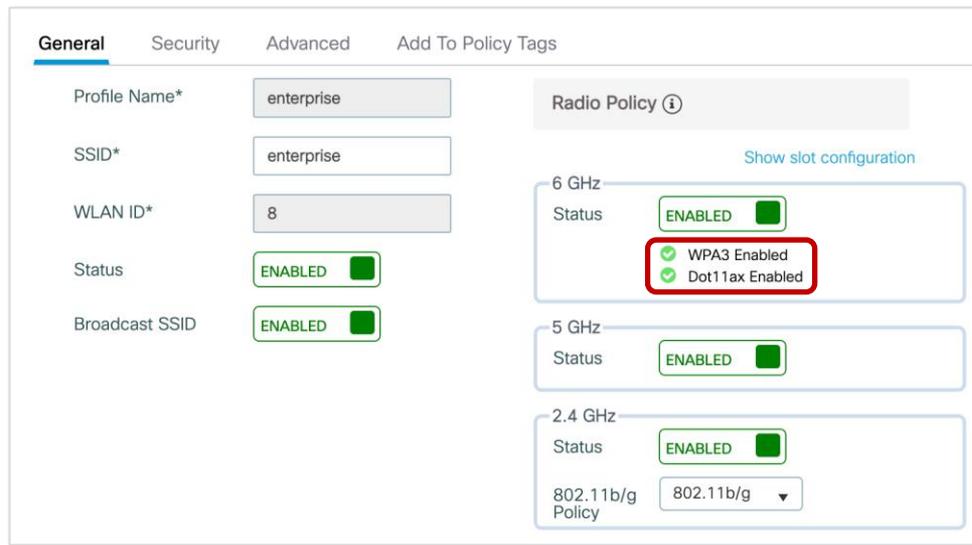


Identity

OpenRoaming



Wi-Fi 6E Security



WPA3 and OWE are **mandatory** for Wi-Fi 6E



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

Wi-Fi 6E Security



WPA3 and OWE are **mandatory** for Wi-Fi 6E

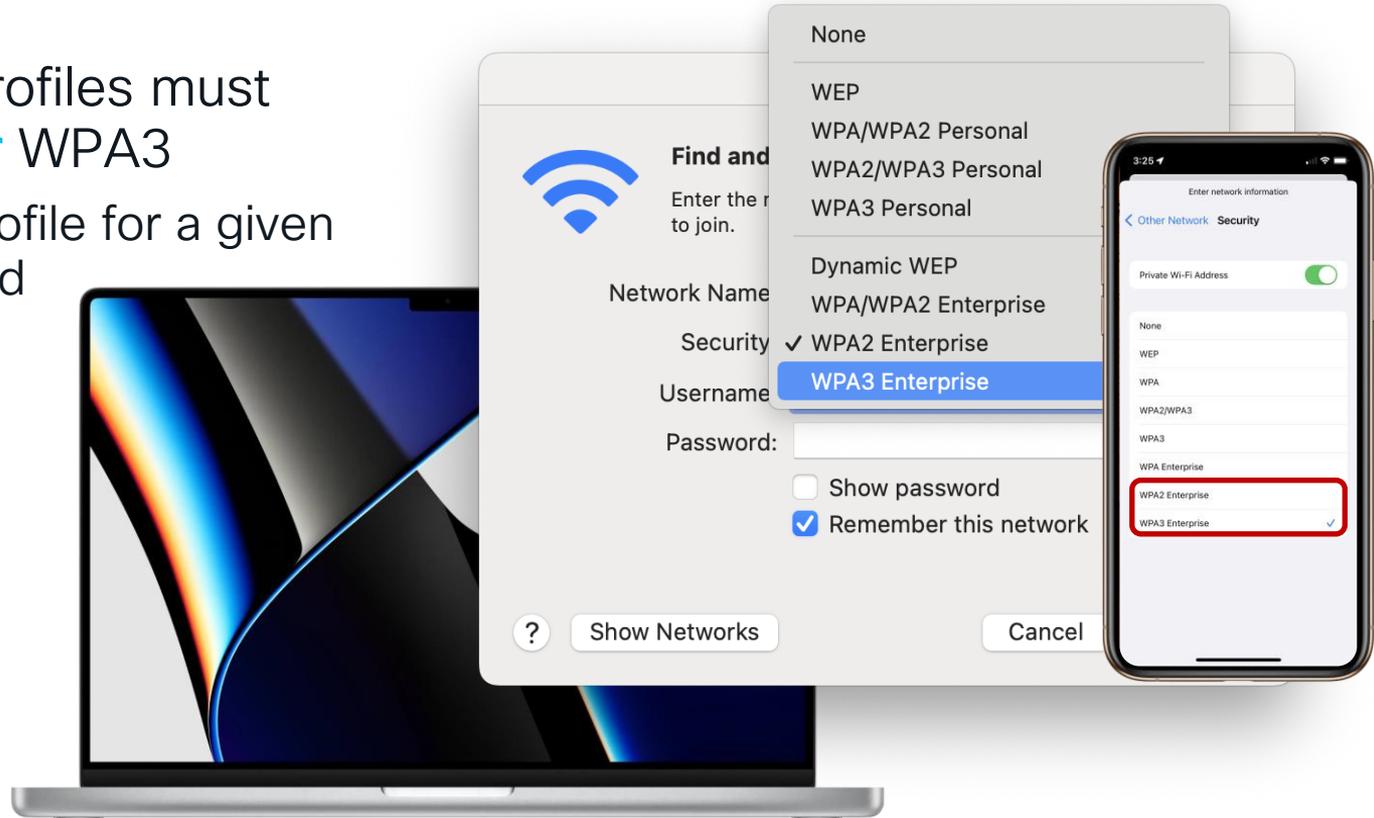


WPA2 and Open are **not** supported on 6GHz

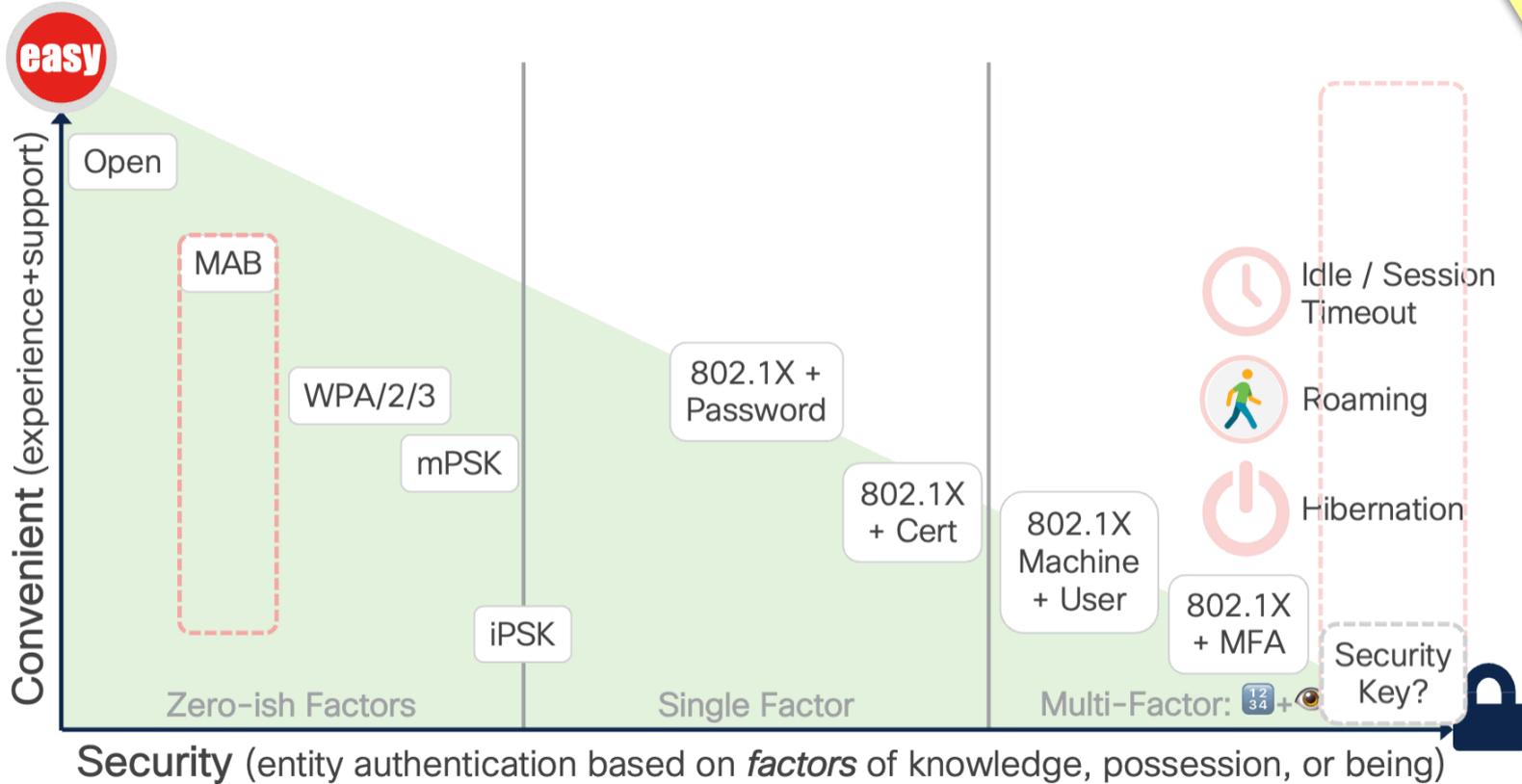
The screenshot displays the configuration interface for a Wi-Fi profile. The 'General' tab is selected, showing 'Profile Name*' as 'enterprise' and 'SSID*' as 'enterprise'. The 'Security' tab is active, showing 'Layer2' settings. The 'WPA2 + WPA3' radio button is selected. The 'WPA Parameters' section shows 'WPA2 Policy' and 'WPA3 Policy' both checked. The 'Protected Management Frame' section shows 'PMF' selected as 'Optional'.

Wi-Fi 6E Security

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



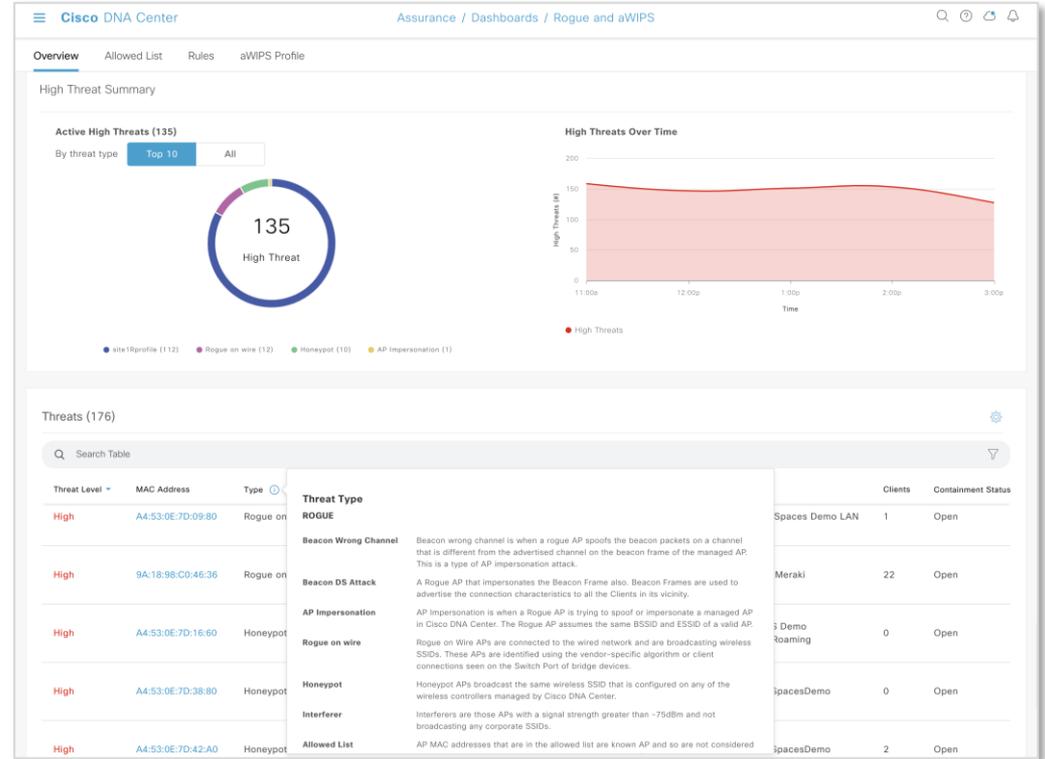
Network Access Security Spectrum



Rogue Detection and Advanced WIPS

Rogue Detection and Advanced WIPS

- Centralized wireless threat management
- Rogue detection
- 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

Rogue Detection and Advanced WIPS

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

The screenshot displays the Cisco DNA Center interface for Rogue and aWIPS management. The main view is titled "Threat 360: Mac A4:53:0E:7D:42:A0".

High Threat Summary: A circular gauge shows 135 High Threats. A legend indicates: site1profile (112), Rogue on wire (12), and Honeypot.

Threats (176): A table lists detected threats with columns for Threat Level, MAC Address, and Type.

Threat Level	MAC Address	Type
High	A4:53:0E:7D:09:80	Rogue on wire
High	9A:18:98:C0:46:36	Rogue on wire
High	A4:53:0E:7D:16:60	Honeypot
High	A4:53:0E:7D:38:80	Honeypot
High	A4:53:0E:7D:42:A0	Honeypot

Threat 360 Details: Threat Level: High, Threat Type: Honeypot, Vendor: Cisco Systems, Inc, Status: Active, Containment Status: Open, Last Reported: Jun 1, 2022 02:06 pm. Location: Global/San Jose/Building 14/Floor1.

Map: A floor plan map shows the location of the threat (SJC14-TME-AP4) and other access points (SJC14-TME-AP1, SJC14-TME-AP2, SJC14-TME-AP3, SJC14-TME-AP7, AP-001).

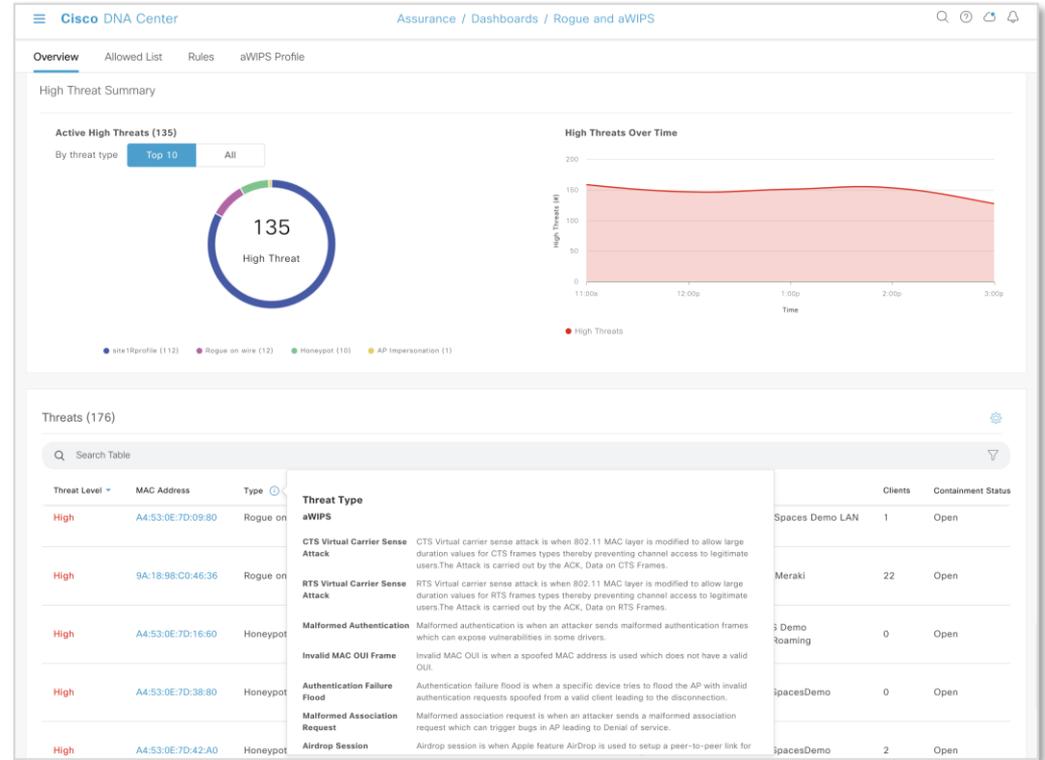
Detections (18): A table lists detected threats with columns for Detecting AP, Detecting AP Site, Adhoc, Rogue SSID, RSSI (dBm), Channels, Radio Type (Band), State, and Last Reported.

Detecting AP	Detecting AP Site	Adhoc	Rogue SSID	RSSI (dBm)	Channels	Radio Type (Band)	State	Last Reported
SJC14-TME-AP9	Global/San Jose/Building 14/Floor1	No	IDNASpacesDemo	-50	11	802.11b/g/n/ax (2.4GHz)	Inactive	Jun 1 01:45
Traffic_Assurance_01	Global/San Jose/Building 14/Floor1	No	DNA Spaces Sensors LAN	-70	11	802.11b/g/n/ax (2.4GHz)	Inactive	Jun 1 02:06
SJC14-TME-AP4	Global/San Jose/Building 14/Floor1	No	IDNASpacesDemo	-71	60	802.11a/n/ac/ax (5GHz)	Active	Jun 1 02:02

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

- Centralized wireless threat management
- Rogue detection
- 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

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

Forensic 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

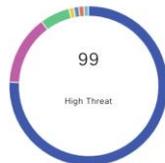
Overview Threats Allowed List Rules aWIPS Profile

Site: Global May 7, 2022 8:26 PM - May 8, 2022 8:26 PM Last 24 hours Refresh Actions

TOTAL ROGUE THREATS	TOTAL AWIPS THREATS	TOTAL UNIQUE ROGUE CLIENTS	ROGUES CONTAINED
197	79	5	7

High Threats Summary

Active High Threats (99)



By Threat Type

Threat Type	Severity	Policy	Status
AP Impersonation	High	Predefined	Active
Association Flood	High	Predefined	Active
Authentic Fuzzed Beacon	High	Predefined	Active
Authentic Fuzzed Probe Request	High	Predefined	Active
Beacon D Fuzzed Probe Response	High	Predefined	Active
Beacon F Honeypot	High	Predefined	Active
Beacon W Interferer	Potential	Predefined	Active
Block Ack Invalid MAC OUI Frame	High	Predefined	Active
Broadcas Malformed Association Request	High	Predefined	Active
CTS Flood Malformed Authentication	High	Predefined	Active
CTS Virtu Neighbor	Informational	Predefined	Active
Deauthen Probe Response Flood	High	Predefined	Active
Deauthen PS Poll Flood	High	Predefined	Active
Disassoci Re-Association Request Flood	High	Predefined	Active
Disassoci Rogue on Wire	High	Predefined	Active
EAPOL Lc RTS Flood	High	Predefined	Active
RTS Virtual Carrier Sense Attack	High	Predefined	Active

Rogue and WIPS Reporting and APIs



The screenshot shows the Cisco DNA Center Reports page. The left sidebar lists various report categories, with 'Rogue and aWIPS' highlighted. The main content area displays two report templates: 'Rogue and aWIPS New Threat' and 'Rogue and aWIPS Threat Detail'. Each template includes a brief description and options to generate the report in CSV, TDE, or JSON format.

The screenshot shows the Cisco DNA Center Platform / Developer Toolkit. The left sidebar lists various API categories, with 'Devices' highlighted. The main content area displays a table of APIs for Rogue and aWIPS.

Method	Name	Description	URL	Actions
GET	Get Allowed Mac Address ^{Intent}	Intent API to fetch all the allowed mac addresses in the system.	/security/threats/rogue/allowed-list	...
POST	Threat Summary ^{Intent}	The Threat Summary for the Rogues and aWIPS	/security/threats/summary	...
GET	Get Threat Types ^{Intent}	Intent API to fetch all threat types defined.	/security/threats/type	...
GET	Get Allowed Mac Address Count ^{Intent}	Intent API to fetch the count of allowed mac addresses in the system.	/security/threats/rogue/allowed-list/count	...
DELETE	Remove Allowed Mac Address ^{Intent}	Intent API to remove the threat mac address from allowed list.	/security/threats/rogue/allowed-list/\${macAddress}	...
POST	Threat Detail Count ^{Intent}	The details count for the Rogue and aWIPS threats	/security/threats/details/count	...
POST	Add Allowed Mac Address ^{Intent}	Intent API to add the threat mac address to allowed list.	/security/threats/rogue/allowed-list	...
GET	Get Threat Levels ^{Intent}	Intent API to fetch all threat levels defined.	/security/threats/level	...
POST	Threat Details ^{Intent}	The details for the Rogue and aWIPS threats	/security/threats/details	...

Access Point Scanning Options



Off-Channel Scanning

- All channels scanned every 180s within a 3m period
- Dwell time is 50ms
- Channel change is 10 ms
- AP is off-channel for 60ms



Monitor Mode Access Point

- Continuous cycle 1200ms dwell across all channels
- Supports Rogue Detection & WIPS, RRM & CleanAir, and Fast Locate



Dedicated Scanning Radio

- Catalyst 9136
- Catalyst 9130
- Catalyst 9120

- Catalyst 9166
- Catalyst 9164
- Catalyst 9162



CleanAir Spectrum Intelligence



- Interferers
 - Layer 1 Denial of Service Attack
- Rogue AP Detection
 - Inverted
 - Invalid Channel
- 6GHz Support
 - Rogue Detection and WIPS

Configuration > Radio Configurations > CleanAir

5 GHz Band | 2.4 GHz Band

General | Trap Configuration

Enable CleanAir

Enable SI

Report Interferers

Available Interference Types

WiFi Inverted
WiFi Invalid Channel

Interference Types to detect

TDD Transmitter
Jammer
Continuous Transmitter
DECT-like Phone

6 GHz Channels 1,200 MHz



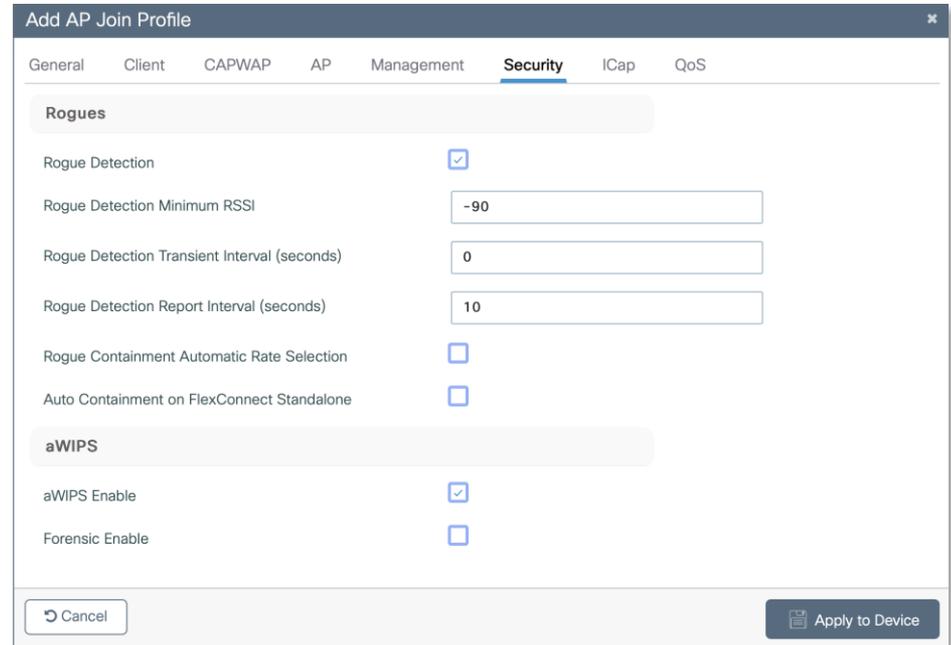
FCC - USA 5950 + 5 X Ch. Number Wavelength 5.1cm - 2.0" to 4.2cm - 1.6"

Low Power Indoor 5dBm/MHz - Net EIRP 18dBm

Radio Band	UNII-5										UNII-6										UNII-7										UNII-8																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																											
Center Freq	5.925	5.975	5.995	6.015	6.035	6.055	6.075	6.095	6.115	6.135	6.155	6.175	6.195	6.215	6.235	6.255	6.275	6.295	6.315	6.335	6.355	6.375	6.395	6.415	6.435	6.455	6.475	6.495	6.515	6.535	6.555	6.575	6.595	6.615	6.635	6.655	6.675	6.695	6.715	6.735	6.755	6.775	6.795	6.815	6.835	6.855	6.875	6.895	6.915	6.935	6.955	6.975	6.995	7.015	7.035	7.055	7.075	7.095	7.115																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																															
20 MHz	1	5	9	13	17	21	25	29	33	37	41	45	49	53	57	61	65	69	73	77	81	85	89	93	97	101	105	109	113	117	121	125	129	133	137	141	145	149	153	157	161	165	169	173	177	181	185	189	193	197	201	205	209	213	217	221	225	229	233																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																															
40 MHz	3	11	19	27	35	43	51	59	67	75	83	91	99	107	115	123	131	139	147	155	163	171	179	187	195	203	211	219	227	235	243	251	259	267	275	283	291	299	307	315	323	331	339	347	355	363	371	379	387	395	403	411	419	427	435	443	451	459	467	475	483	491	499	507	515	523	531	539	547	555	563	571	579	587	595	603	611	619	627	635	643	651	659	667	675	683	691	699	707	715	723	731	739	747	755	763	771	779	787	795	803	811	819	827	835	843	851	859	867	875	883	891	899	907	915	923	931	939	947	955	963	971	979	987	995	1003	1011	1019	1027	1035	1043	1051	1059	1067	1075	1083	1091	1099	1107	1115	1123	1131	1139	1147	1155	1163	1171	1179	1187	1195	1203	1211	1219	1227	1235	1243	1251	1259	1267	1275	1283	1291	1299	1307	1315	1323	1331	1339	1347	1355	1363	1371	1379	1387	1395	1403	1411	1419	1427	1435	1443	1451	1459	1467	1475	1483	1491	1499	1507	1515	1523	1531	1539	1547	1555	1563	1571	1579	1587	1595	1603	1611	1619	1627	1635	1643	1651	1659	1667	1675	1683	1691	1699	1707	1715	1723	1731	1739	1747	1755	1763	1771	1779	1787	1795	1803	1811	1819	1827	1835	1843	1851	1859	1867	1875	1883	1891	1899	1907	1915	1923	1931	1939	1947	1955	1963	1971	1979	1987	1995	2003	2011	2019	2027	2035	2043	2051	2059	2067	2075	2083	2091	2099	2107	2115	2123	2131	2139	2147	2155	2163	2171	2179	2187	2195	2203	2211	2219	2227	2235	2243	2251	2259	2267	2275	2283	2291	2299	2307	2315	2323	2331	2339	2347	2355	2363	2371	2379	2387	2395	2403	2411	2419	2427	2435	2443	2451	2459	2467	2475	2483	2491	2499	2507	2515	2523	2531	2539	2547	2555	2563	2571	2579	2587	2595	2603	2611	2619	2627	2635	2643	2651	2659	2667	2675	2683	2691	2699	2707	2715	2723	2731	2739	2747	2755	2763	2771	2779	2787	2795	2803	2811	2819	2827	2835	2843	2851	2859	2867	2875	2883	2891	2899	2907	2915	2923	2931	2939	2947	2955	2963	2971	2979	2987	2995	3003	3011	3019	3027	3035	3043	3051	3059	3067	3075	3083	3091	3099	3107	3115	3123	3131	3139	3147	3155	3163	3171	3179	3187	3195	3203	3211	3219	3227	3235	3243	3251	3259	3267	3275	3283	3291	3299	3307	3315	3323	3331	3339	3347	3355	3363	3371	3379	3387	3395	3403	3411	3419	3427	3435	3443	3451	3459	3467	3475	3483	3491	3499	3507	3515	3523	3531	3539	3547	3555	3563	3571	3579	3587	3595	3603	3611	3619	3627	3635	3643	3651	3659	3667	3675	3683	3691	3699	3707	3715	3723	3731	3739	3747	3755	3763	3771	3779	3787	3795	3803	3811	3819	3827	3835	3843	3851	3859	3867	3875	3883	3891	3899	3907	3915	3923	3931	3939	3947	3955	3963	3971	3979	3987	3995	4003	4011	4019	4027	4035	4043	4051	4059	4067	4075	4083	4091	4099	4107	4115	4123	4131	4139	4147	4155	4163	4171	4179	4187	4195	4203	4211	4219	4227	4235	4243	4251	4259	4267	4275	4283	4291	4299	4307	4315	4323	4331	4339	4347	4355	4363	4371	4379	4387	4395	4403	4411	4419	4427	4435	4443	4451	4459	4467	4475	4483	4491	4499	4507	4515	4523	4531	4539	4547	4555	4563	4571	4579	4587	4595	4603	4611	4619	4627	4635	4643	4651	4659	4667	4675	4683	4691	4699	4707	4715	4723	4731	4739	4747	4755	4763	4771	4779	4787	4795	4803	4811	4819	4827	4835	4843	4851	4859	4867	4875	4883	4891	4899	4907	4915	4923	4931	4939	4947	4955	4963	4971	4979	4987	4995	5003	5011	5019	5027	5035	5043	5051	5059	5067	5075	5083	5091	5099	5107	5115	5123	5131	5139	5147	5155	5163	5171	5179	5187	5195	5203	5211	5219	5227	5235	5243	5251	5259	5267	5275	5283	5291	5299	5307	5315	5323	5331	5339	5347	5355	5363	5371	5379	5387	5395	5403	5411	5419	5427	5435	5443	5451	5459	5467	5475	5483	5491	5499	5507	5515	5523	5531	5539	5547	5555	5563	5571	5579	5587	5595	5603	5611	5619	5627	5635	5643	5651	5659	5667	5675	5683	5691	5699	5707	5715	5723	5731	5739	5747	5755	5763	5771	5779	5787	5795	5803	5811	5819	5827	5835	5843	5851	5859	5867	5875	5883	5891	5899	5907	5915	5923	5931	5939	5947	5955	5963	5971	5979	5987	5995	6003	6011	6019	6027	6035	6043	6051	6059	6067	6075	6083	6091	6099	6107	6115	6123	6131	6139	6147	6155	6163	6171	6179	6187	6195	6203	6211	6219	6227	6235	6243	6251	6259	6267	6275	6283	6291	6299	6307	6315	6323	6331	6339	6347	6355	6363	6371	6379	6387	6395	6403	6411	6419	6427	6435	6443	6451	6459	6467	6475	6483	6491	6499	6507	6515	6523	6531	6539	6547	6555	6563	6571	6579	6587	6595	6603	6611	6619	6627	6635	6643	6651	6659	6667	6675	6683	6691	6699	6707	6715	6723	6731	6739	6747	6755	6763	6771	6779	6787	6795	6803	6811	6819	6827	6835	6843	6851	6859	6867	6875	6883	6891	6899	6907	6915	6923	6931	6939	6947	6955	6963	6971	6979	6987	6995	7003	7011	7019	7027	7035	7043	7051	7059	7067	7075	7083	7091	7099	7107	7115	7123	7131	7139	7147	7155	7163	7171	7179	7187	7195	7203	7211	7219	7227	7235	7243	7251	7259	7267	7275	7283	7291	7299	7307	7315	7323	7331	7339	7347	7355	7363	7371	7379	7387	7395	7403	7411	7419	7427	7435	7443	7451	7459	7467	7475	7483	7491	7499	7507	7515	7523	7531	7539	7547	7555	7563	7571	7579	7587	7595	7603	7611	7619	7627	7635	7643	7651	7659	7667	7675	7683	7691	7699	7707	7715	7723	7731	7739	7747	7755	7763	7771	7779	7787	7795	7803	7811	7819	7827	7835	7843	7851	7859	7867	7875	7883	7891	7899	7907	7915	7923	7931	7939	7947	7955	7963	7971	7979	7987	7995	8003	8011	8019	8027	8035	8043	8051	8059	8067	8075	8083	8091	8099	8107	8115	8123	8131	8139	8147	8155	8163	8171	8179	8187	8195	8203	8211	8219	8227	8235	8243	8251	8259	8267	8275	8283	8291	8299	8307	8315	8323	8331	8339	8347	8355	8363	8371	8379	8387	8395	8403	8411	8419	8427	8435	8443	8451	8459	8467	8475	8483	8491	8499	8507	8515	8523	8531	8539	8547	8555	8563	8571	8579	8587	8595	8603	8611	8619	8627	8635	8643	8651	8659	8667	8675	8683	8691	8699	8707	8715	8723	8731	8739	8747	8755	8763	8771	8779	8787	8795	8803	8811	8819	8827	8835	8843	8851	8859	8867	8875	8883	8891	8899	8907	8915	8923	8931	8939	8947	8955	8963	8971	8979	8987	8995	9003	9011	9019	9027	9035	9043	9051	9059	9067	9075	9083	9091	9099	9107	9115	9123	9131	9139	9147	9155	9163	9171	9179	9187	9195	9203	9211	9219	9227	9235	9243	9251	9259	9267	9275	9283	9291	9299	9307	9315	9323	9331	9339	9347	9355	9363	9371	9379	9387	9395	9403	9411	9419	9427	9435	9443	9451	9459	9467	9475	9483	9491	9499	9507	9515	9523	9531	9539	954

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



The screenshot shows the 'Add AP Join Profile' configuration window with the 'Security' tab selected. The window contains the following settings:

Setting	Value
Rogue Detection	<input checked="" type="checkbox"/>
Rogue Detection Minimum RSSI	-90
Rogue Detection Transient Interval (seconds)	0
Rogue Detection Report Interval (seconds)	10
Rogue Containment Automatic Rate Selection	<input type="checkbox"/>
Auto Containment on FlexConnect Standalone	<input type="checkbox"/>
aWIPS	
aWIPS Enable	<input checked="" type="checkbox"/>
Forensic Enable	<input type="checkbox"/>

Buttons: Cancel, Apply to Device

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
- Detecting APs on the wired network is hard
 - Wired 802.1x matters

The screenshot shows the 'Add AP Join Profile' configuration window, specifically the 'Security' tab. The 'Rogues' section is expanded, showing 'Rogue Detection' checked. 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. The 'Rogue Policies' tab is selected, and the 'Rogue AP Rules' sub-tab is active. In the 'General' section, 'Rogue Detection Security Level' is set to 'Custom', 'Expiration timeout for Rogue APs (seconds)*' is 1200, 'Validate Rogue Clients against AAA' is unchecked, 'Validate Rogue APs against AAA' is unchecked, 'Rogue Polling Interval (seconds)' is 3600, 'Detect and Report Adhoc Networks' is checked, 'Rogue Detection Client Number Threshold*' is 0, 'Rogue Init Timer (seconds)*' is 180, 'AP Authentication' is unchecked, 'AP Authentication Alarm Threshold*' is 1, and 'Syslog Notification' is unchecked. In the 'Auto Contain' section, 'Auto Containment Level' is 1, 'Auto Containment only for Monitor Mode APs' is unchecked, 'Using our SSID' is checked and highlighted with a red box, 'Valid client on Rogue AP' is unchecked, and 'Adhoc Rogue AP' is unchecked. The 'MFP Configuration' section shows 'Global MFP State' and 'AP Impersonation Detection' are unchecked, and 'MFP Key Refresh Interval (hours)*' is 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

The screenshot shows the configuration page for Wireless Protection Policies, specifically the Rogue Policies tab. The page is divided into two main sections: General and Auto Contain. The General section includes settings for Rogue Detection Security Level (set to Custom), Expiration timeout for Rogue APs (1200), Validate Rogue Clients against AAA (checked), Validate Rogue APs against AAA (unchecked), Rogue Polling Interval (3600), Detect and Report Adhoc Networks (checked), Rogue Detection Client Number Threshold (0), Rogue Init Timer (180), AP Authentication (unchecked), AP Authentication Alarm Threshold (1), and Syslog Notification (unchecked). The Auto Contain section includes settings for Auto Containment Level (1), Auto Containment only for Monitor Mode APs (unchecked), Using our SSID (unchecked), Valid client on Rogue AP (unchecked), Adhoc Rogue AP (unchecked), and MFP Configuration (Global MFP State unchecked, AP Impersonation Detection unchecked, MFP Key Refresh Interval 24 hours).

Cisco DNA Center 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 Rules

- Create Rogue Rules to classify rogues as Malicious or Friendly based on specific criteria
 - SSID name
 - RSSI value
 - Encryption condition
 - Minimum rogue client count
- Rules can also define actions
 - Alert
 - Contain

The image displays three overlapping screenshots of the 'Edit Rogue AP Rule' configuration interface. The top window shows the 'Rule Name' field set to 'malicious' and the 'Rule Type' dropdown menu open, with 'Malicious' selected. A yellow sticky note with the text 'FYI' is placed over the top right corner of this window. The middle window shows the 'State' dropdown menu open, with 'Contain' selected, and the 'Match Operation' dropdown menu open, with 'Contain' selected. The bottom window shows the 'Match Operation' dropdown menu set to 'Any' and the 'Add Condition' dropdown menu open, with 'ssid' selected.

Rogue Notification Triggers



- The Catalyst 9800 has aggressive rogue notification thresholds by default
- In environments with a large number of Rogues, this may result in excessive notifications sent to the receiver
- In these scenarios, increase the Rogue AP and Client RSSI notification threshold
 - The default value is 0
 - Recommendation to increase to 5 or higher

```
C9800 (config) #wireless wps rogue ap notify-rssi-deviation 5
C9800 (config) #wireless wps rogue clients notify-rssi-deviation 5
```

Rogue AP Containment

- How do we contain Rogue APs?
 - Containment is a spoofed 802.11 disassociation/deauthentication request attack

The screenshot displays the Cisco DNA Center interface for managing Rogue APs. The main view shows details for Threat 360 (Mac A4:53:0E:7C:99:E0), which is a High Threat Honeypot from Cisco Systems, Inc. The interface includes a map of the location (Global/San Jose/Building 14/Floor1) with several APs (SJC14-TME-AP1 through AP-0001) and their status. A red box highlights the 'Start Containment' button in the Actions menu. Below the map, there are sections for 'Detections (28)' and 'Clients (4)'. The 'Detections' table lists several entries with columns for Detecting AP, Detecting AP Site, Adhoc, Rogue SSID, RSSI (dBm), Channels, Radio Type (Band), State, and Time.

Detecting AP	Detecting AP Site	Adhoc	Rogue SSID	RSSI (dBm)	Channels	Radio Type (Band)	State	Time
SJC14-TME-AP6	Global/San Jose/Building 14/Floor1	No	IDNAS Demo OpenRoaming	-71	11	802.11b/g/n/ax (2.4GHz)	Inactive	Jun 1 01:25
SJC14-TME-AP4	Global/San Jose/Building 14/Floor1	No	IDNA Spaces Demo LAN	-72	44	802.11a/n/ac/ax (5GHz)	Active	Jun 1 02:37
SJC14-TME-AP4	Global/San Jose/Building 14/Floor1	No	IDNASpacesDemo	-72	44	802.11a/n/ac/ax (5GHz)	Active	Jun 1 02:44

Rogue AP Containment

- How do we contain Rogue APs?
 - Containment is a spoofed 802.11 disassociation/deauthentication request attack

The screenshot displays the Cisco DNA Center interface for Rogue and aWIPS. A warning dialog is open, titled "Warning", with a yellow triangle icon. The text reads: "Using this feature may have legal consequences. Wireless containment will be initiated for the below rogue BSSIDs on wireless controller with IP address 172.20.224.95. Do you want to continue?". Below the text, there is a "Rogue BSSID" label and two input fields containing the MAC addresses "A4:53:0E:7C:99:E0" and "A4:53:0E:7C:99:E3". At the bottom of the dialog, there are "No" and "Yes" buttons. The background interface shows a table of threats and a table of APs.

Threat Level	Threat Type	Vendor	Status	Containment S...	Last Reported
High	Honeypot	Cisco Systems, Inc	Active	Open	Jun 1, 2022 02:48 pm

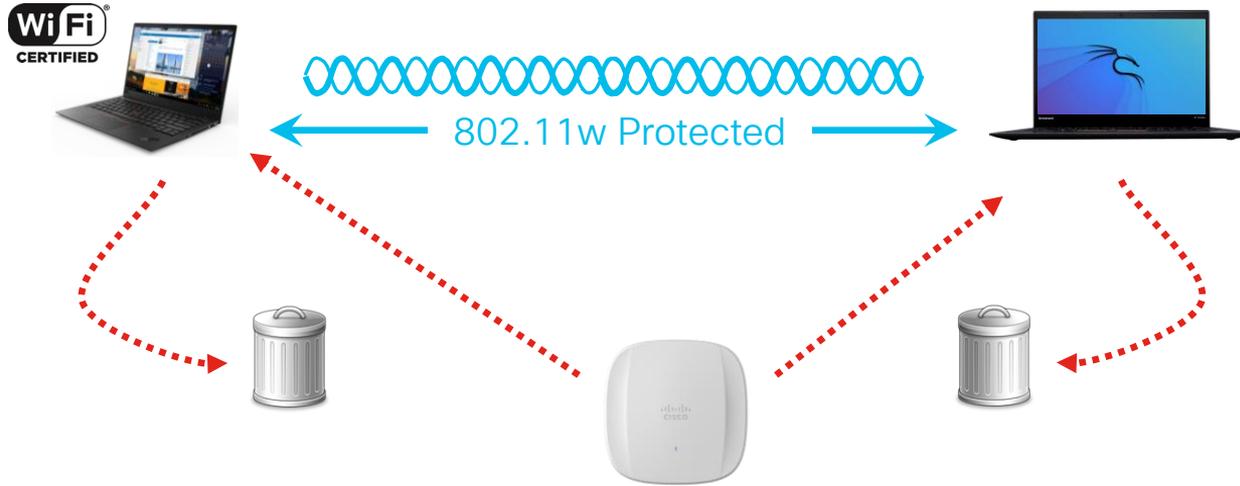
SSID (dflm)	Channels	Radio Type (Band)	State					
SJC14-TME-AP6	Global/San Jose/Building 14/Floor1	No	IDNAS Demo OpenRoaming	-71	11	802.11b/g/n/ax (2.4GHz)	Inactive	Jun 1 01:25
SJC14-TME-AP4	Global/San Jose/Building 14/Floor1	No	IDNA Spaces Demo LAN	-72	44	802.11a/n/ac/ax (5GHz)	Active	Jun 1 02:37
SJC14-TME-AP4	Global/San Jose/Building 14/Floor1	No	IDNASpacesDemo	-72	44	802.11a/n/ac/ax (5GHz)	Active	Jun 1 02:44

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 for Rogue and aWIPS. It shows a list of threats, with two specific threat details windows open. The first window shows a threat with a high level, identified as a Honeypot from Cisco Systems, Inc. A warning message is displayed: "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". The second window shows a threat with a potential level, identified as an Interferer from UNKNOWN, with an active status and open containment. Below the threat details is a floor plan for Global/San Jose/Building 14/Floor1, showing the physical location of the rogue AP (SJC14-TME-AP2) and other access points (SJC14-TME-AP3, SJC14-TME-AP4, AP-0001).

Rogue Containment with WPA3



Rogue AP Auto Containment

- While we can configure the network to automatically contain detect Rogue APs, consider your environment and how to ensure that **only** malicious Rogues are being contained

Configuration > Security > Wireless Protection Policies

Rogue Policies | Rogue AP Rules | Client Exclusion Policies

Auto Contain [Apply]

General

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:

AP Authentication Alarm Threshold*: 1

Syslog Notification:

Auto Containment

Auto Containment Level: 1

Auto Containment only for Monitor Mode APs:

Using our SSID:

Valid client on Rogue AP:

Adhoc Rogue AP:

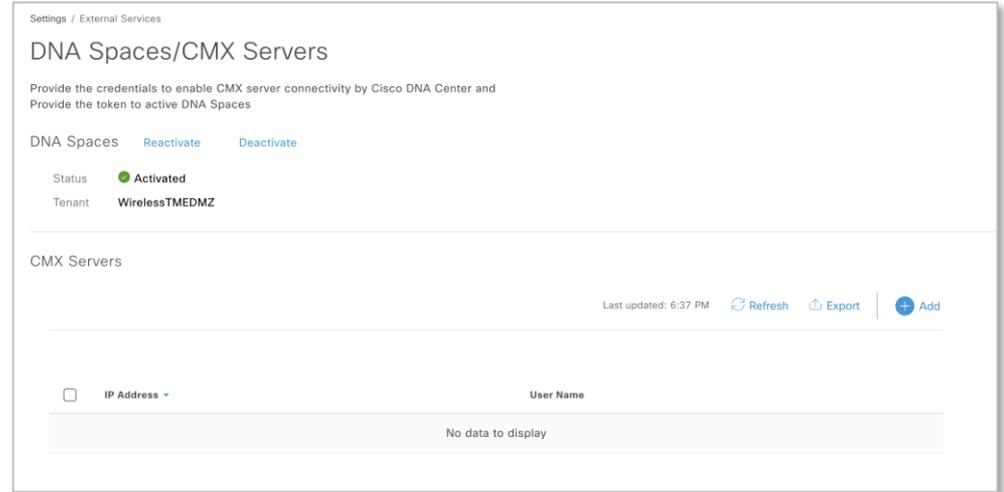
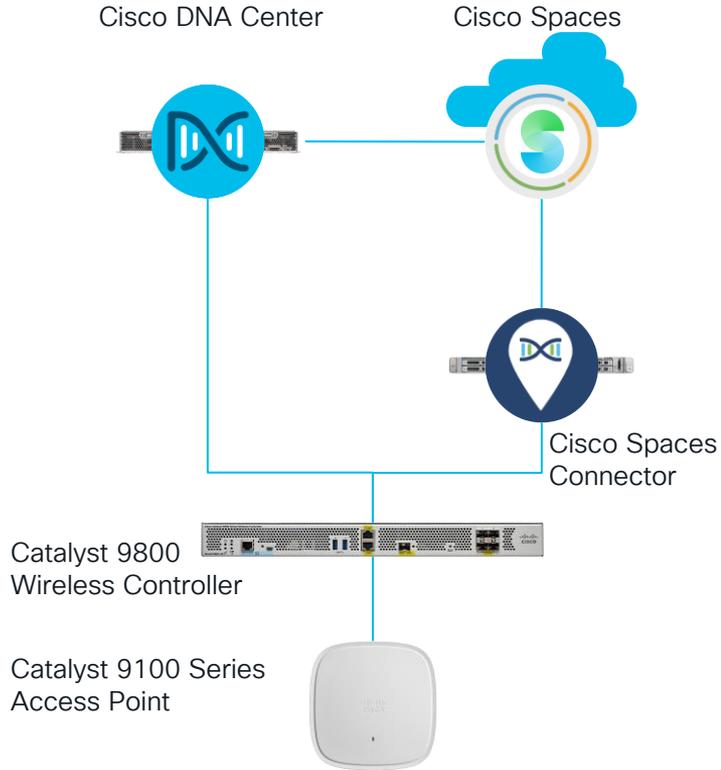
MFP Configuration

Global MFP State:

AP Impersonation Detection:

MFP Key Refresh Interval (hours)*: 24

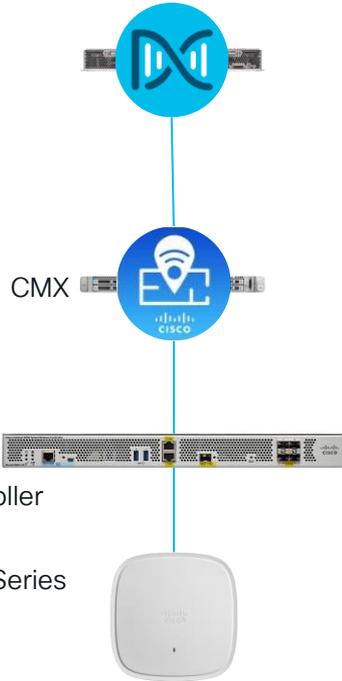
Enabling Location Services



Enabling Location Services



Cisco DNA Center



Catalyst 9800
Wireless Controller

Catalyst 9100 Series
Access Point

The screenshot shows the 'Settings / External Services' page in Cisco DNA Center. The main section is titled 'DNA Spaces/CMX Servers' and includes instructions: 'Provide the credentials to enable CMX server connectivity by Cisco DNA Center and Provide the token to active DNA Spaces'. Below this, there are tabs for 'DNA Spaces' with 'Reactivate' and 'Deactivate' options. The 'Status' is 'Activated' (indicated by a green dot) and the 'Tenant' is 'WirelessTMEDMZ'. A table for 'CMX Servers' is shown with a 'Last updated:' column and a 'No data to display' message. A modal window titled 'Add CMX Server' is open on the right, containing fields for 'IP Address*', 'User Name*', 'Password*', 'SSH User Name*', and 'SSH Password*'. 'Cancel' and 'Add' buttons are at the bottom of the modal.

Rogue on Wire

- Matching Algorithms
 - MAC Address $\pm 3/\pm 2/\pm 1$
 - Vendor matching algorithms

The screenshot displays the Cisco DNA Center interface for a specific threat. The main header shows 'Threat 360: Mac 6A:3A:0E:53:A6:E9'. Below this, a table lists threat details:

Threat Level	Threat Type	Vendor	Status	Containment S...	Last Reported
High	Rogue on wire	UNKNOWN	Active	Open	Jun 5, 2022 03:23 pm

A floor plan diagram shows the location: Global/San Jose/Building 14/Floor1. A table below the diagram lists 'Switch Port Detail (1)' with the following data:

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

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

The screenshot displays the Cisco DNA Center interface for a threat analysis. The main view is titled "Threat 360: Mac 6A:3A:0E:53:A6:E9". It shows a "High Threat Summary" with 14 active high threats, categorized by type: "Rogue on wire" (12) and "Honeypot" (1). A circular gauge indicates the total of 14 high threats. Below this, a "Threats (134)" section provides a search table for threats, with the top entry being a "High" threat with MAC address 68:3A:1E:53:A6:E0, identified as "Rogue on wire".

The right-hand pane shows a detailed view of the threat, including a floor plan of the location (Global/San Jose/Building 14/Floor1) with a red circle highlighting a specific area. Below the floor plan, a "Switch Port Detail (1)" section shows "Detections (9)" and "Clients (19)". A table of clients is displayed, with the "Clients (19)" count highlighted in a red box. The table lists MAC addresses, gateway MACs, rogue AP MACs, IP addresses, and last heard times.

MAC Address	Gateway MAC	Rogue AP MAC	IP Address	Last Heard
70:F3:5A:7B:FD:F1	6A:3A:0E:53:A6:E9	6A:3A:0E:53:A6:E9	10.70.0.100	Jun 5, 2022 03:23 pm
70:F3:5A:7B:FD:31	6A:3A:0E:53:A6:E9	6A:3A:0E:53:A6:E9	10.70.0.90	Jun 5, 2022 03:23 pm
70:F3:5A:7B:FC:11	6A:3A:0E:53:A6:E9	6A:3A:0E:53:A6:E9	10.70.0.99	Jun 5, 2022 03:14 pm
70:F3:5A:7B:FA:11	6A:3A:0E:53:A6:E9	6A:3A:0E:53:A6:E9	10.70.0.80	Jun 5, 2022 03:23 pm
70:F3:5A:7B:F9:71	6A:3A:0E:53:A6:E9	6A:3A:0E:53:A6:E9	10.70.0.105	Jun 5, 2022 03:23 pm

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

Cisco DNA Center Assurance / Dashboards / Rogue and aWIPS

Threat 360: Mac 6A:3A:0E:53:A6:E9

Threat Level	Threat Type	Vendor	Status	Containment S...	Actions
High	Rogue on wire	UNKNOWN	Active	Open	Shutdown Switchport Add to Allowed list

Location: Global/San Jose/Building 14/Floor1

Threats (134)

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

Switch Port Detail (1) | Detections (9) | Clients (19)

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

Securing AP Switch Port Access



802.1x
← Authentication (EAP-FAST) →

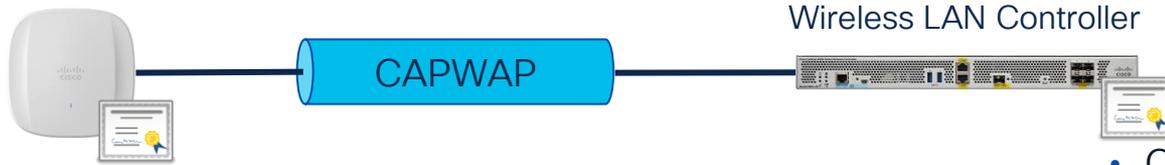


How do we bootstrap configure the AP?

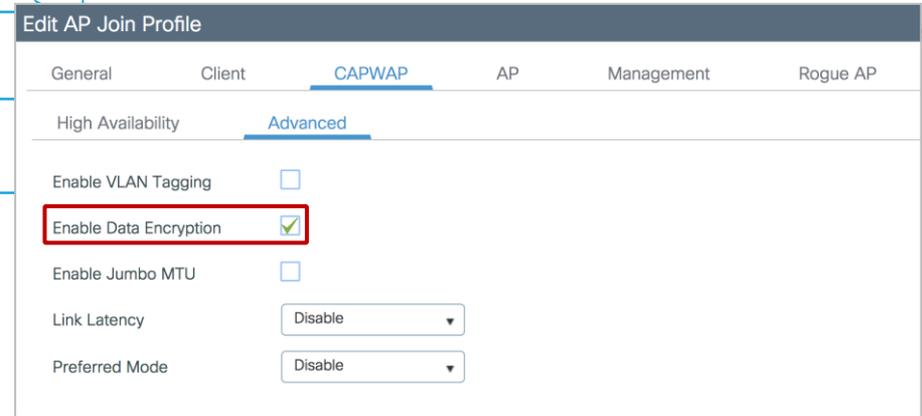
- Pre-Provision before deploying the APs
- Enable 802.1x after bringing up the wireless network

The screenshot shows the 'Add AP Join Profile' configuration window with the 'Management' tab selected. Under the 'Credentials' section, there are three fields: 'Dot1x Username' with a text input field containing 'Enter dot1x Username', 'Dot1x Password' with a text input field containing 'Enter Dot1x Password', and 'Dot1x Password Type' with a dropdown menu set to 'clear'. At the bottom, there are 'Cancel' and 'Apply to Device' buttons.

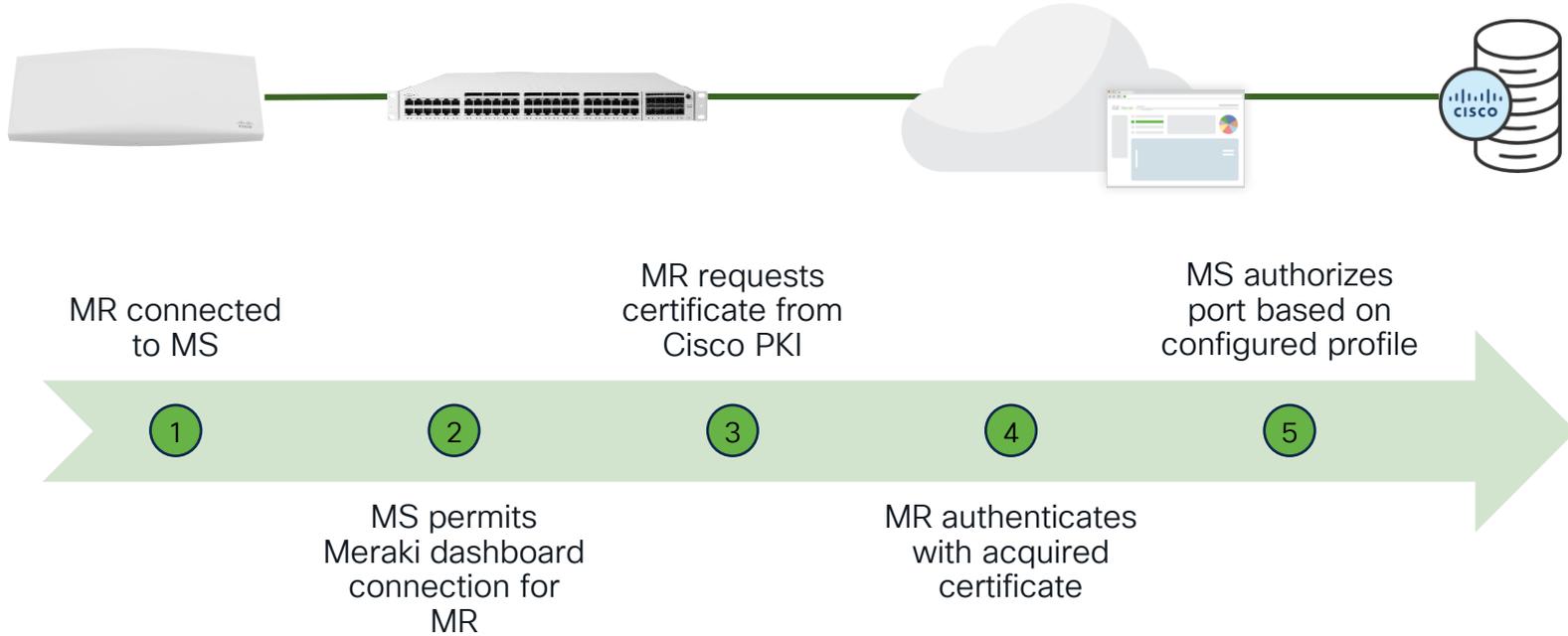
Securing AP to Controller Communication



- CAPWAP Control encrypted by default
- CAPWAP Data encapsulated but not encrypted by default



SecurePort



Air Marshal

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



MSE WIPS End of Life



WIPS service on MSE is declared as EoL from 11th May 2022 onwards.

- MSE platform had already been declared EoL in Nov 2018.
- MSE 8.x had already been declared EoL Aug 2018.
- All the PIDs corresponding to WIPS license would be EoL.
- The EoL is applicable to all the MSE 7.x and 8.x releases



Next Steps

- NextGen aWIPS solution is available with DNA Center and WLC 9800 with DNA-A license.
- No separate local mode or monitor mode licenses are required for APs.
- High touch escalation support based on customer needs is available.

Product ID	Product Description
AIR-LM-WIPS-*	Cisco Enhanced Local Mode wIPS License
AIR-WIPS-*	Cisco wIPS License
C1-MSE-WIPS-*	Cisco ONE Mobility Svcs
L-LM-WIPS-*	Wireless IPS Lic For Enhanced Local Mode AP- E Delivery
L-MM-WIPS-*	Wireless IPS Lic For Monitor Mode AP- E Delivery
L-WIPS-*	WIPS Monitor Mode and Enhanced Local Mode licenses
MSE-WIPS-*	MSE WIPS Tracker Term

Cisco DNA Center Security Advisories



Tools / Security Advisories

Click [here](#) to access customized security advisories based on your device configuration, powered by CX Cloud.

ADVISORIES: 2 Critical, 39 High, 28 Medium

SCAN CRITERIA: 5 Software Version, 0 Custom, 0 Advanced

Re-scan Network

Settings

Devices (64)

Device Name	IP Address	Advisories	Platform	Image Version
ASR1K_TME.ASR1K_TME	172.20.224.132	69	C1111-8P	16.9.4
SJC14F1-WTME-C9K-48UXM.cisco.com	172.20.224.109	69	C9300-48UXM	16.9.4
c9800-40-TMEDNAC.cisco.com	172.20.224.55	0	C9800-40-K9	17.8.1
SpacesWLC	172.20.226.210	0	C9800-CL-K9	17.9.20220411:075
Spirent_WLC.cisco.com	172.20.224.56	0	C9800-40-K9	17.7.20210815:031

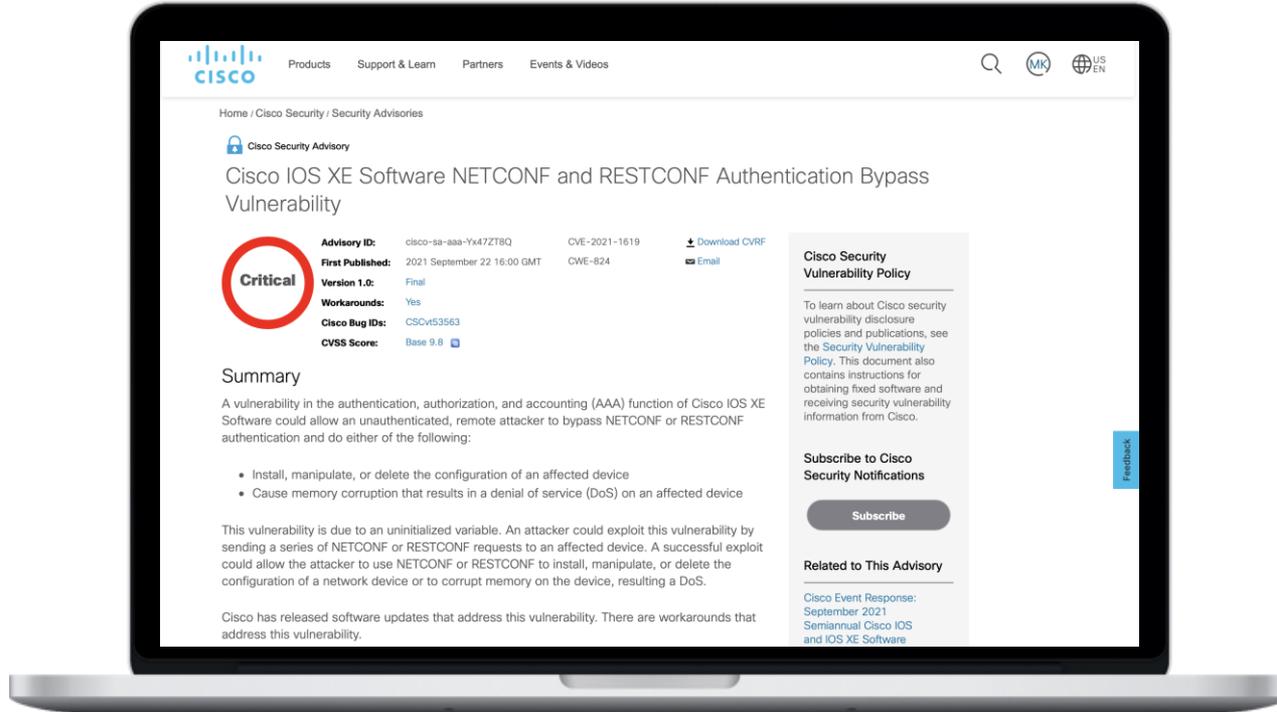
Cisco DNA Center Security Advisories



The screenshot displays the Cisco DNA Center interface for Security Advisories. The left sidebar shows a summary of advisories (2 Critical, 39 High, 28 Medium) and a list of devices (64). The main content area shows details for device SJC14F1-WTME-C9K-48UXM.cisco.com (172.20.224.109), which is reachable and has an uptime of 25 days 7 hrs 10 mins. A table lists 69 advisories, with the following details highlighted:

Advisory ID	Advisory Title	CVSS Score	Impact	Fix Version
cisco-sa-aaa-Yx47ZT8Q	Cisco IOS XE Software NETCONF and RESTCONF Authentication Bypass Vulnerability	9.8	Critical	16.9.8
cisco-sa-telnetd-EFJrEzPx	Telnet Vulnerability Affecting Cisco Products: June 2020	9.8	High	16.9.6
cisco-sa-ioxPE-KgGvCAf9	Cisco IOx for IOS XE Software Privilege Escalation Vulnerability	9.8	Critical	N/A

Cisco DNA Center Security Advisories



Cisco DNA Center Security Advisories



Affected Products

Vulnerable Products

This vulnerability affects Cisco IOS XE Software if it is running in autonomous or controller mode and Cisco IOS XE SD-WAN Software. For either to be affected, all of the following must be configured:

- AAA
- NETCONF, RESTCONF, or both
- **enable password** without **enable secret**

For information about which Cisco software releases are vulnerable, see the [Fixed Software](#) section of this advisory.

Note: The standalone Cisco IOS XE SD-WAN release images are separate from the universal Cisco IOS XE Software releases. The SD-WAN feature set was first integrated into the universal Cisco IOS XE Software releases starting with IOS XE Software Release 17.2.1r. For additional information, see the [Install and Upgrade Cisco IOS XE Release 17.2.1r and Later](#) chapter of the [Cisco SD-WAN Getting Started Guide](#).

Determine the Device Configuration

To determine whether a device has a vulnerable configuration, do the following:

Check AAA Configuration

To determine whether AAA authentication is configured on the device, use the **show running-config | include aaa authentication login** command, as shown in the following example:

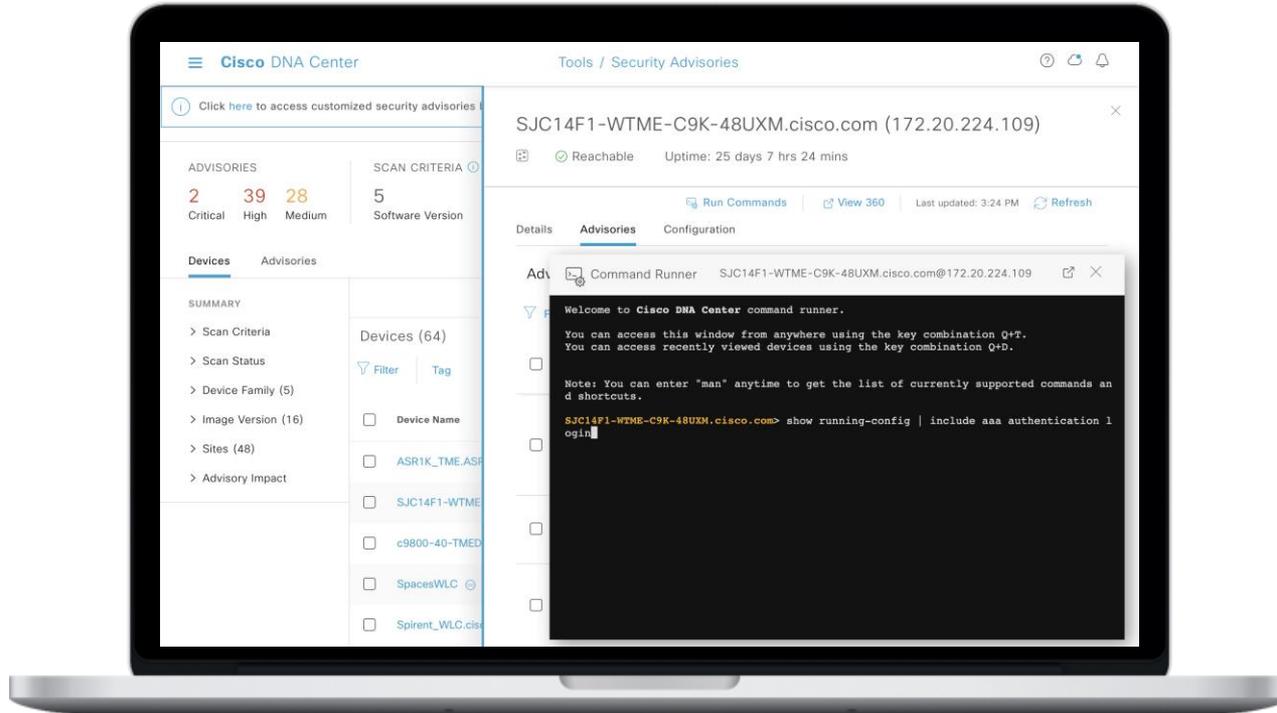
```
Router#show running-config | include aaa authentication login
aaa authentication login default local group example
Router#
```

5 star 0
4 star 0
3 star 0
2 star 0
1 star 0

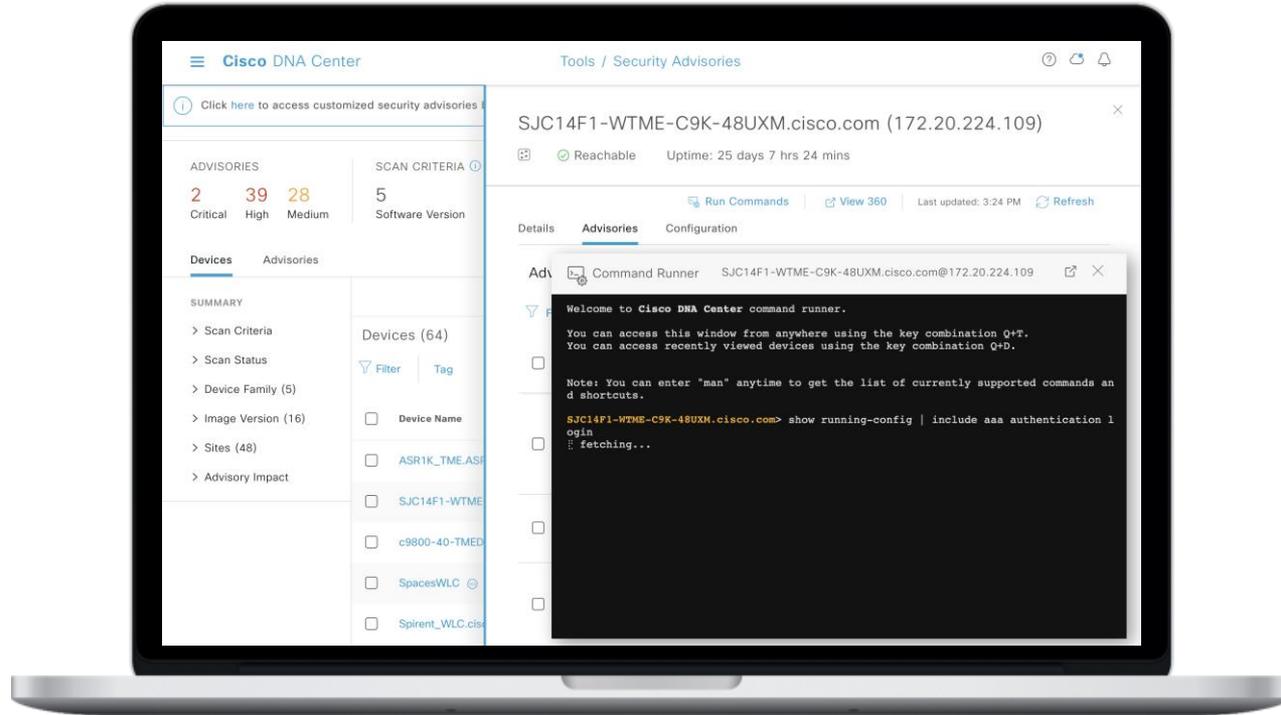
Leave additional feedback

Feedback

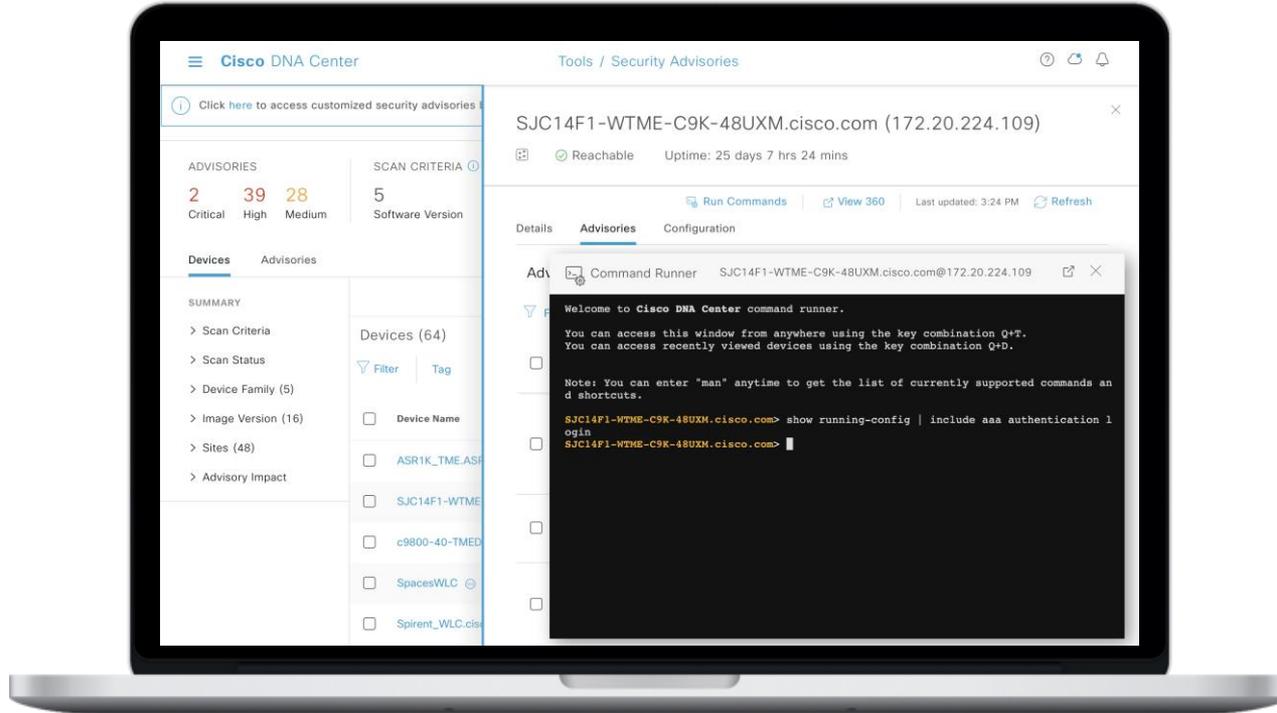
Cisco DNA Center Security Advisories



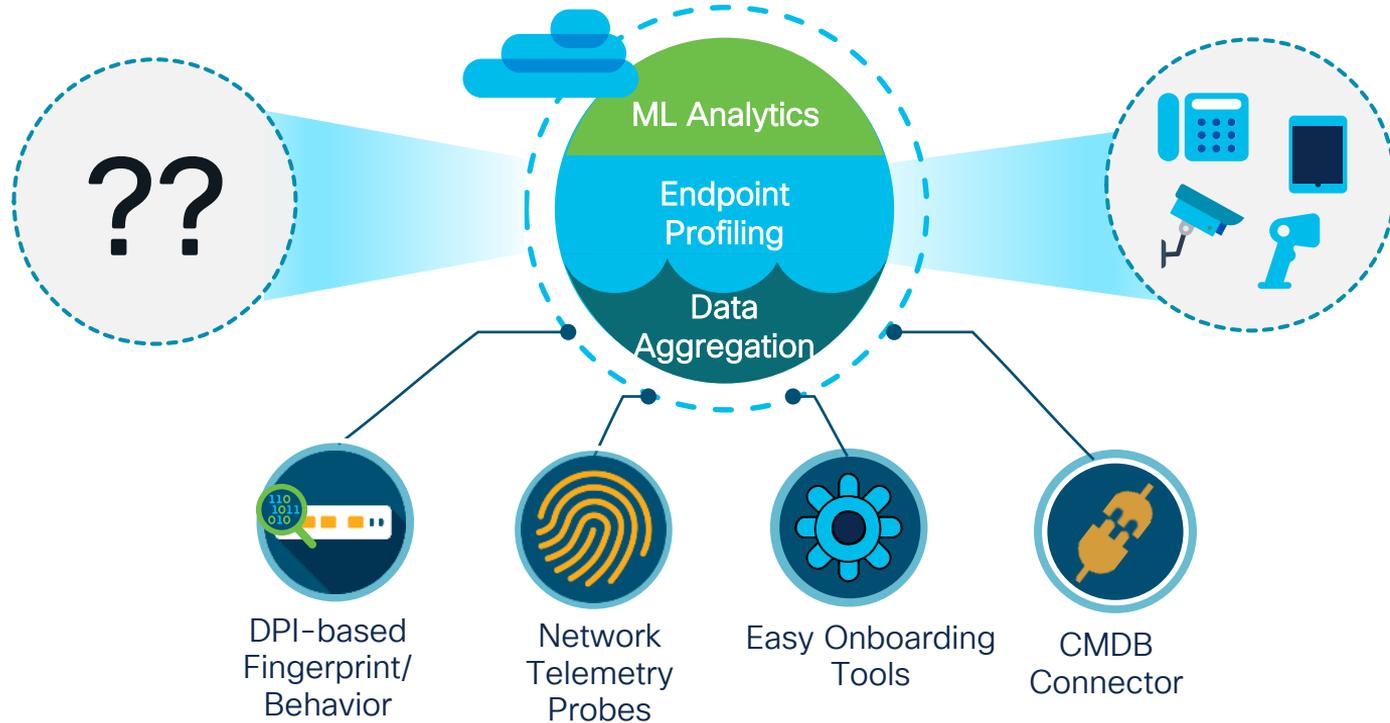
Cisco DNA Center Security Advisories



Cisco DNA Center Security Advisories



Cisco DNA Center AI Endpoint Analytics



Network as a Sensor

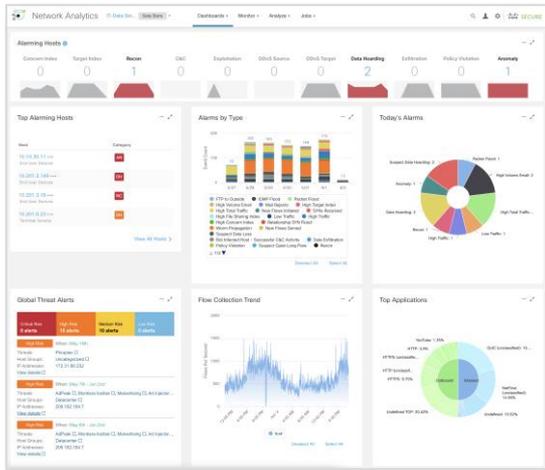
Secure Network Analytics Integration



Netflow



Malware detection and cryptographic compliance on Cisco Stealthwatch



Top Security Events for 10.201.3.18

Security Event	Count	Concern Index	First Active	Target Host	Target Host Group	Actions
Port Scan - 49195	50	546,000	06/02 3:51:05 PM	10.201.0.16	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	...

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**

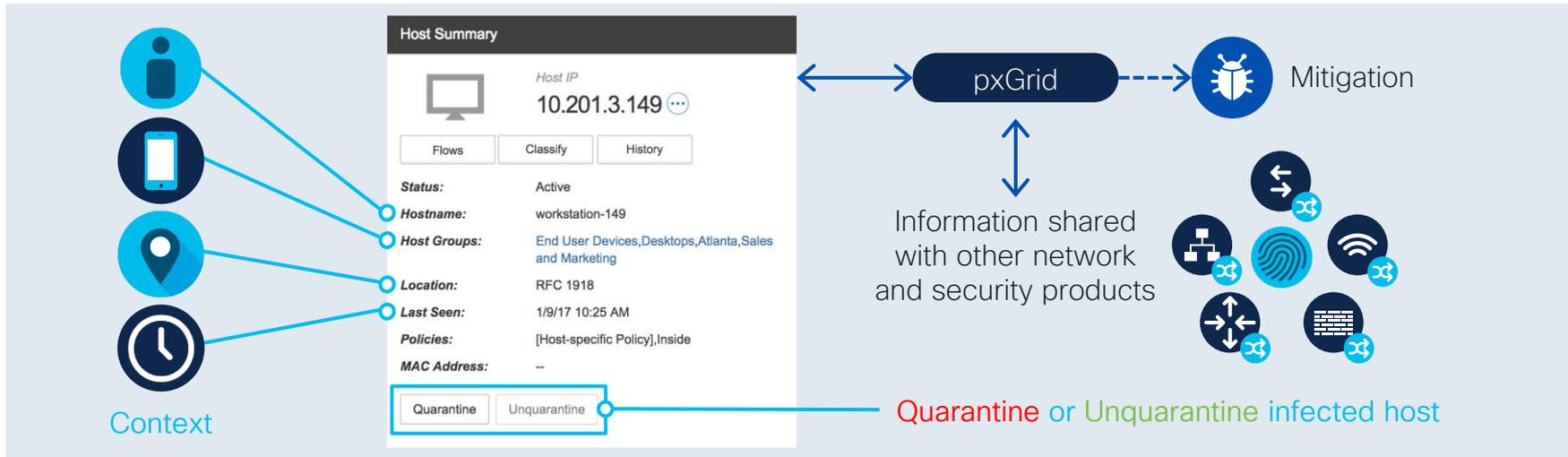
MITRE Techniques: **Exfiltration Over Alternative Protocol**

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



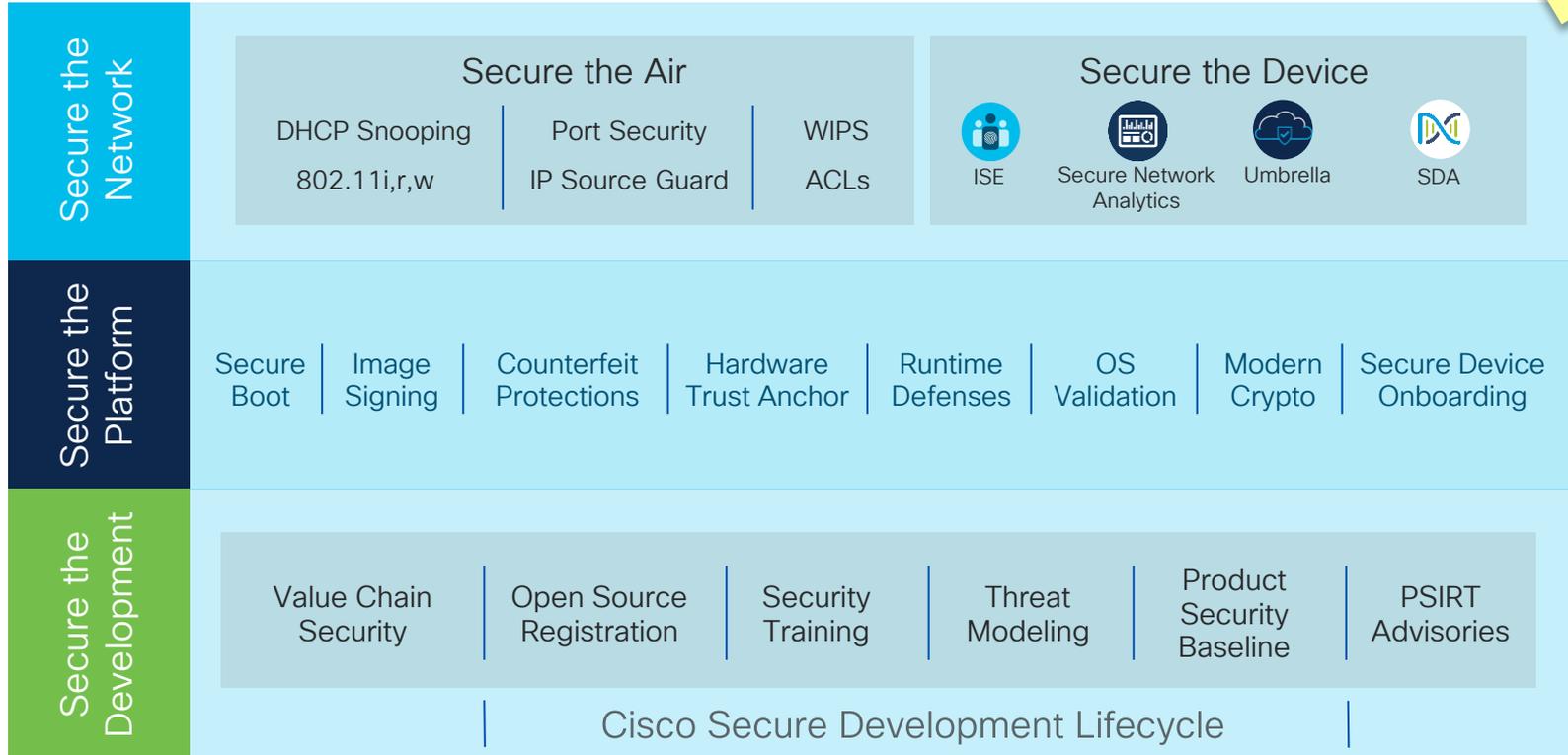
Secure the Devices



Secure the Network



Trustworthy Systems





The bridge to possible

Thank you

CISCO *Live!*

#CiscoLive

Fill out your session surveys!



Attendees who fill out a minimum of four session surveys and the overall event survey will get **Cisco Live-branded socks** (while supplies last)!



Attendees will also earn 100 points in the **Cisco Live Challenge** for every survey completed.



These points help you get on the leaderboard and increase your chances of winning daily and grand prizes

Continue your education

CISCO *Live!*

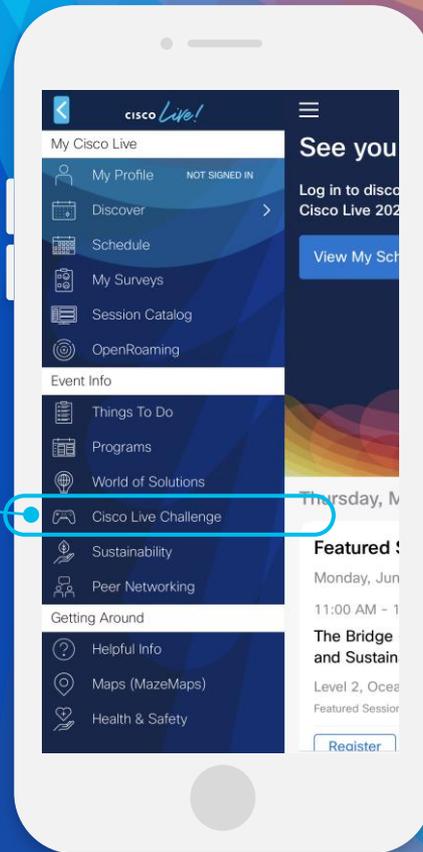
- Visit the Cisco Showcase for related demos
- Book your one-on-one Meet the Engineer meeting
- Attend the interactive education with DevNet, Capture the Flag, and Walk-in Labs
- Visit the On-Demand Library for more sessions at www.CiscoLive.com/on-demand

Cisco Live Challenge

Gamify your Cisco Live experience!
Get points for attending this session!

How:

- 1 Open the Cisco Events App.
- 2 Click on 'Cisco Live Challenge' in the side menu.
- 3 Click on View Your Badges at the top.
- 4 Click the + at the bottom of the screen and scan the QR code:



The Cisco Live! logo features the word "CISCO" in a bold, black, sans-serif font, followed by "Live!" in a black, cursive script font. The background is a vibrant, multi-colored abstract pattern of overlapping, wavy bands in shades of red, orange, yellow, green, and blue, radiating from a bright white center on the right side.

CISCO *Live!*

Let's go

#CiscoLive