

cisco *Live!*

Let's go



The bridge to possible

Understanding Wireless Security

And the Implications for Secure Wireless Network Design

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

Agenda

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



Wireless Security Fundamentals

Securing the Wireless Network



Secure the
Air



Secure the
Devices



Secure the
Network

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

Tal Arad, CISO and Head of Technology, Carlsberg

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

Wireless Attack Surface

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

Wireless Protected Access

WPA

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

WPA2

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

Authentication Mechanisms

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

WPA3

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



WPA3

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

802.11 Fundamentals

Authentication



802.11 Fundamentals

Authentication



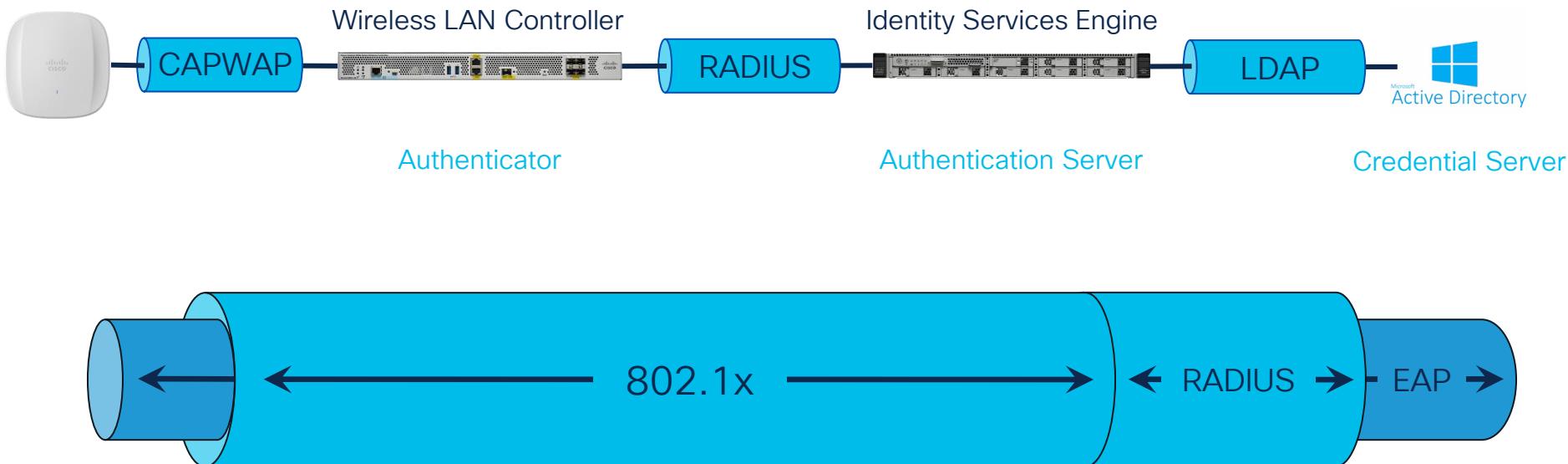
802.11 Fundamentals

Authentication



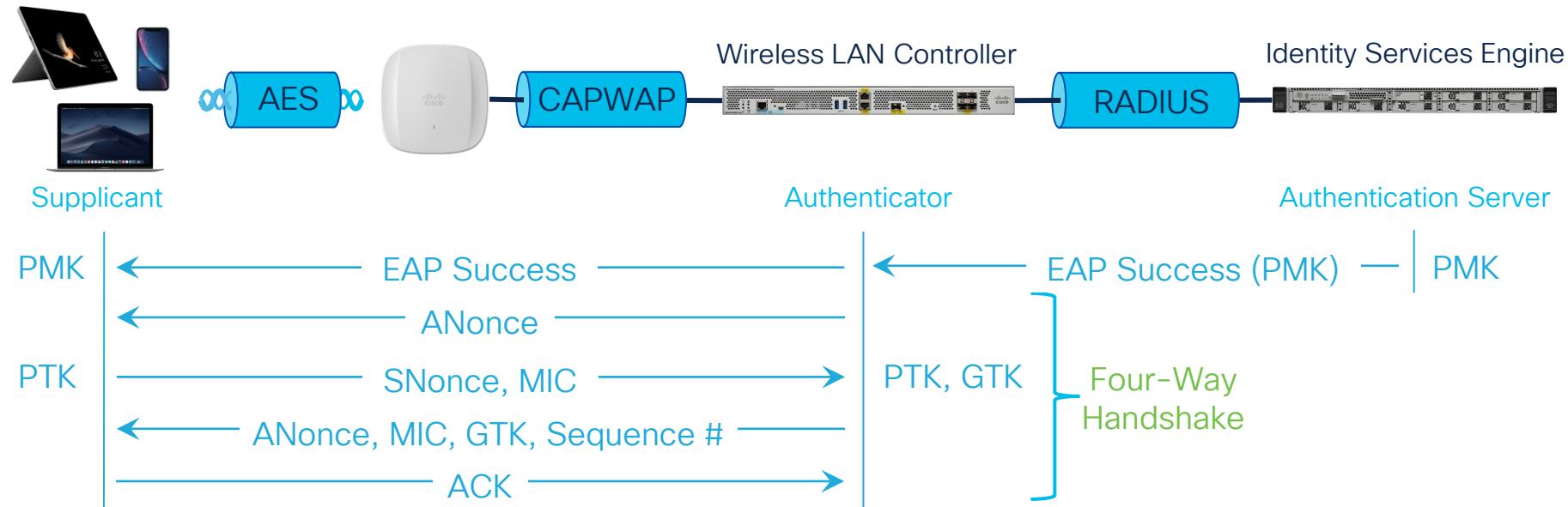
802.11 Fundamentals

Authentication



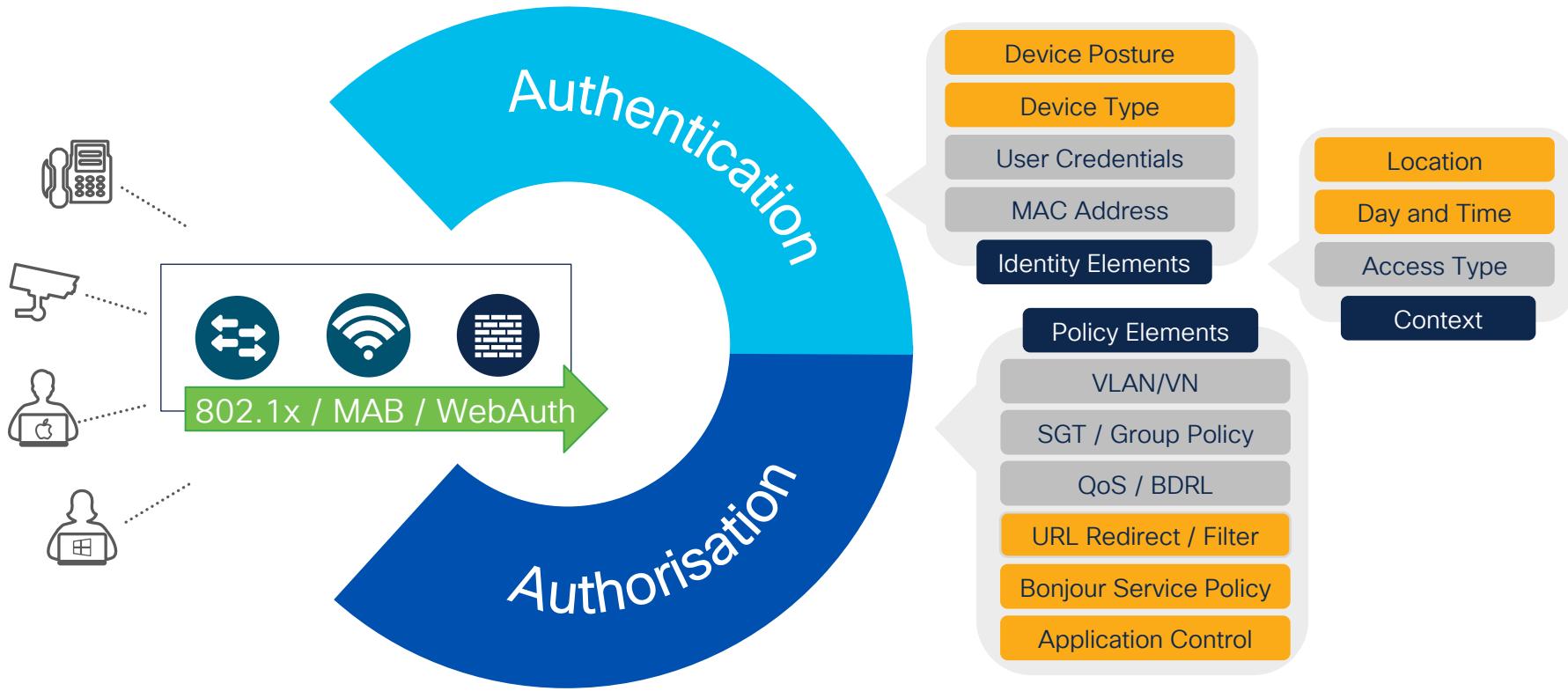
802.11 Fundamentals

Encryption



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

Authentication and Authorisation

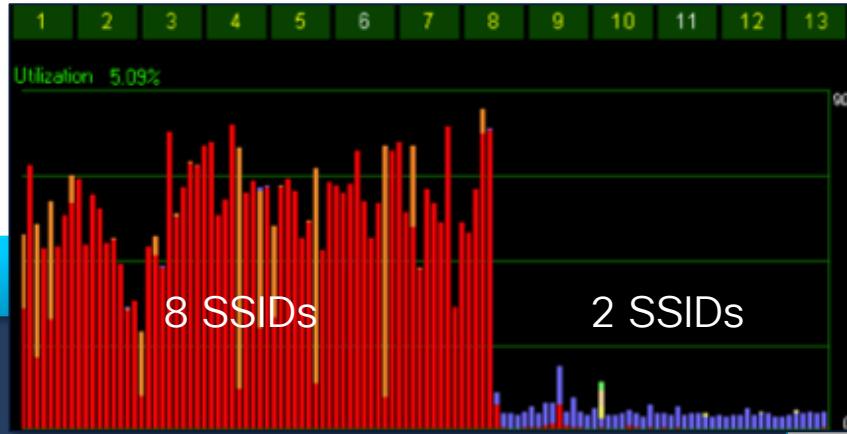


Authorisation

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)

Secure Fast Roaming Challenges



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

Secure Fast Roaming

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



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

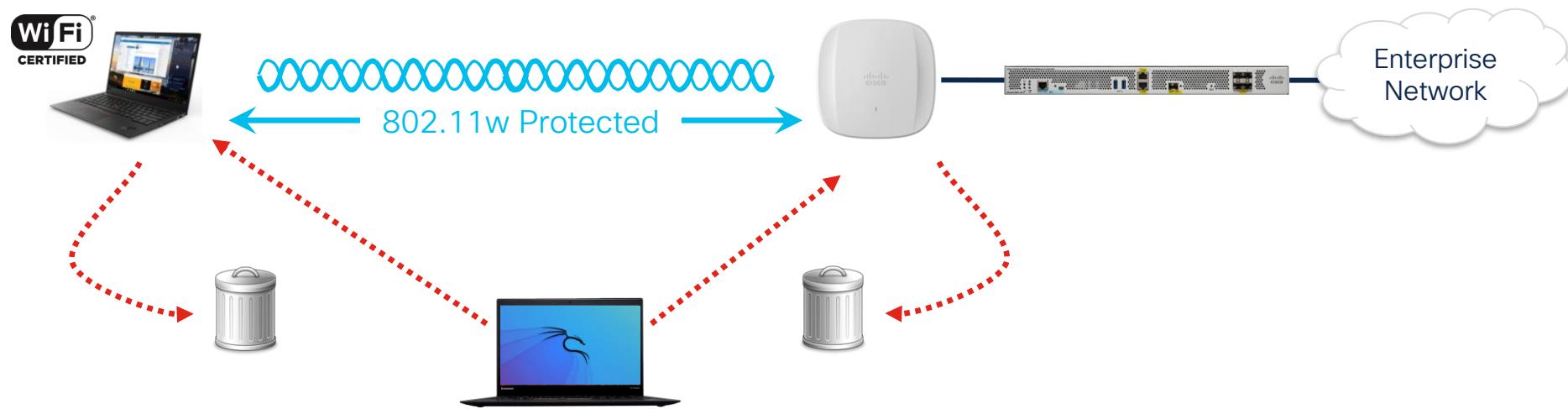
Key Reinstallation Attack



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

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

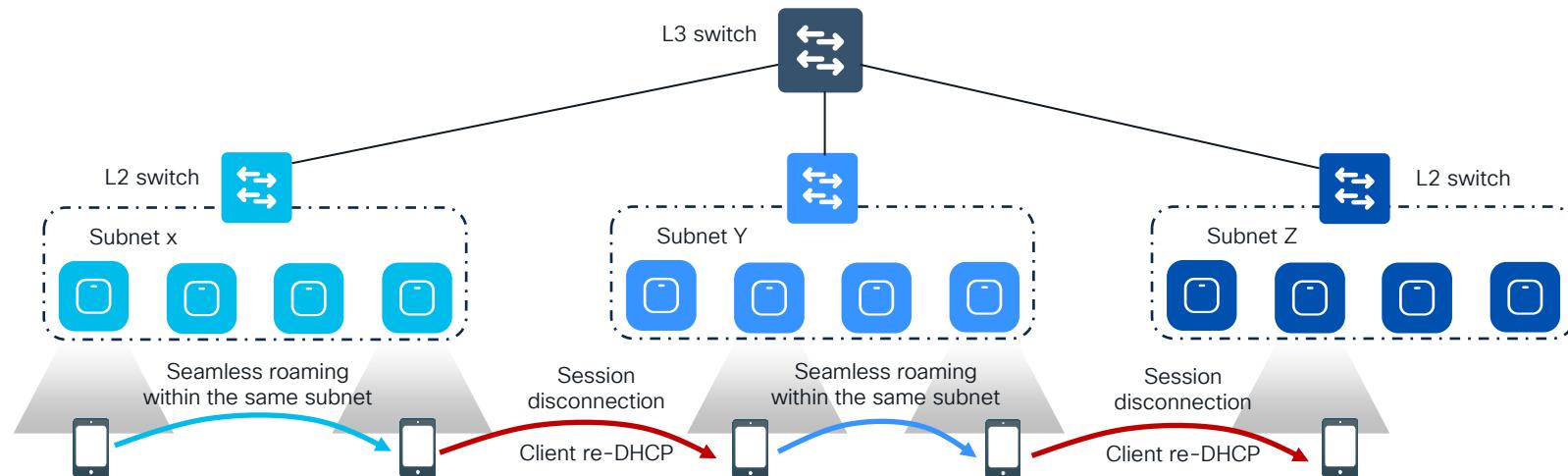
802.11w Protected Management Frames



Seamless Roaming at Scale

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

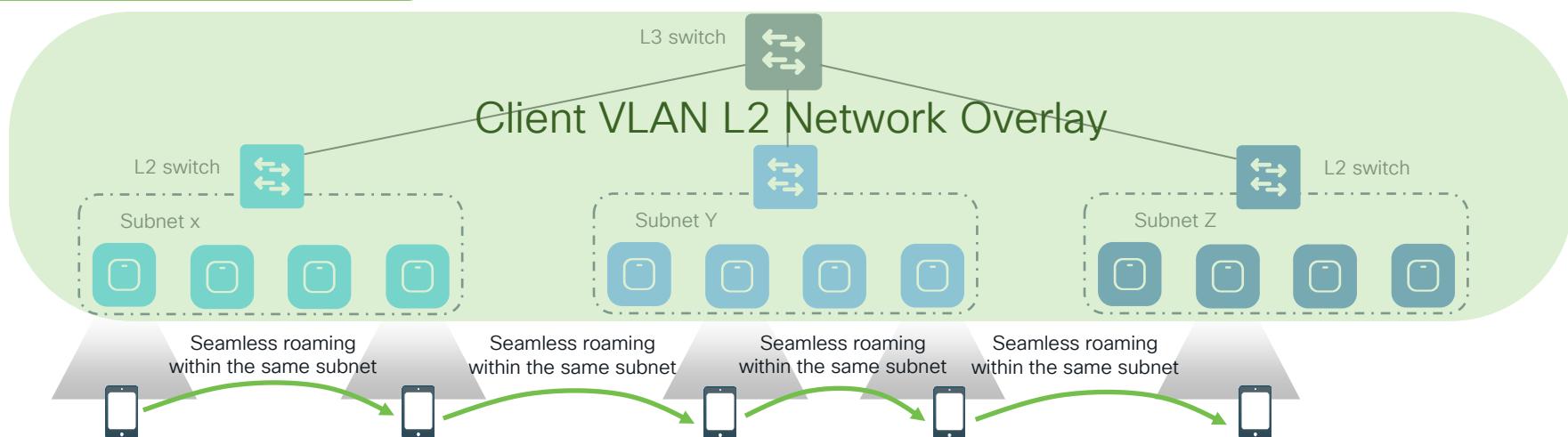
Large broadcast domains do not
scale and is counter to networking
best practice



Seamless Roaming at Scale

For L3 seamless roaming an extended VLAN network overlay is required

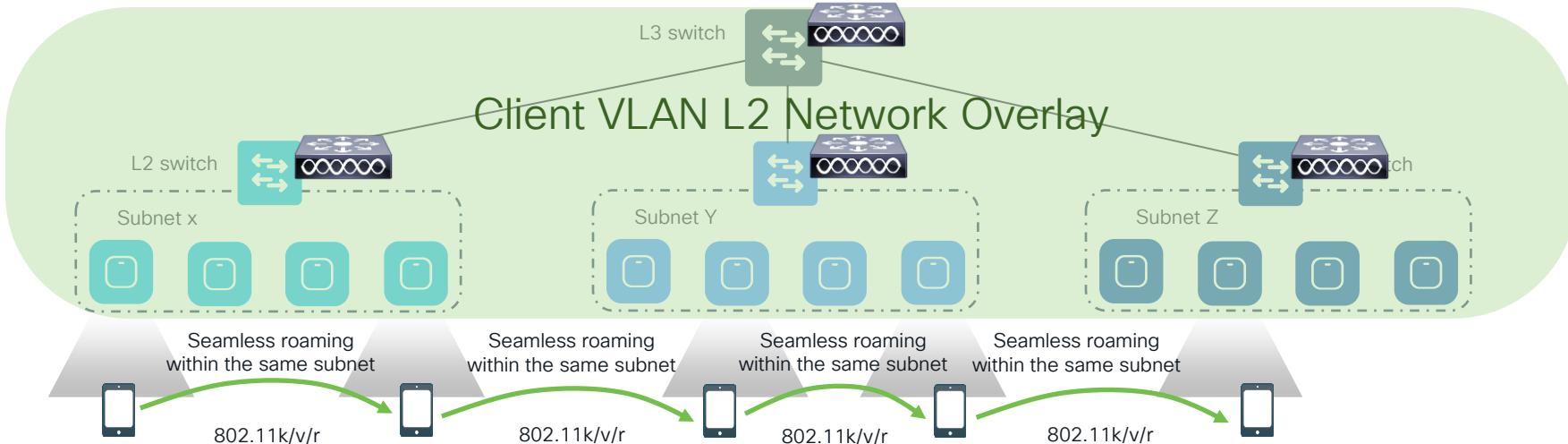
A data termination point is required to roam across L3 boundaries



Seamless Roaming at Scale

Edge Wireless Service
Data Plane (DP) Termination

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



On-Prem and Cloud Identity



On-Prem Identity



802.1x, Network Access



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



Cloud Identity

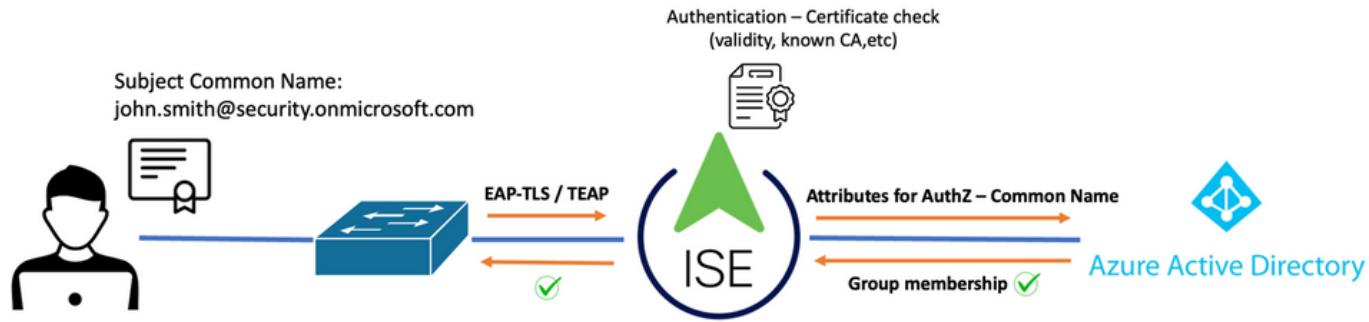
VPN, Application Access



SAMLv2, OpenID Connect



Cloud Identity with EAP-TLS



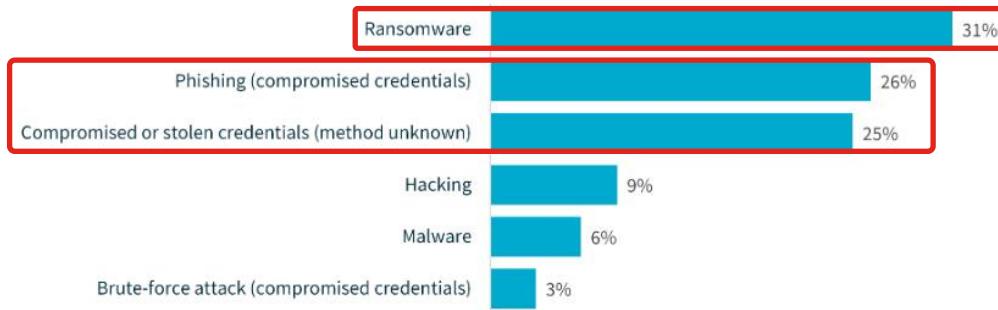
Multi-Factor Authentication



Zero Trust

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

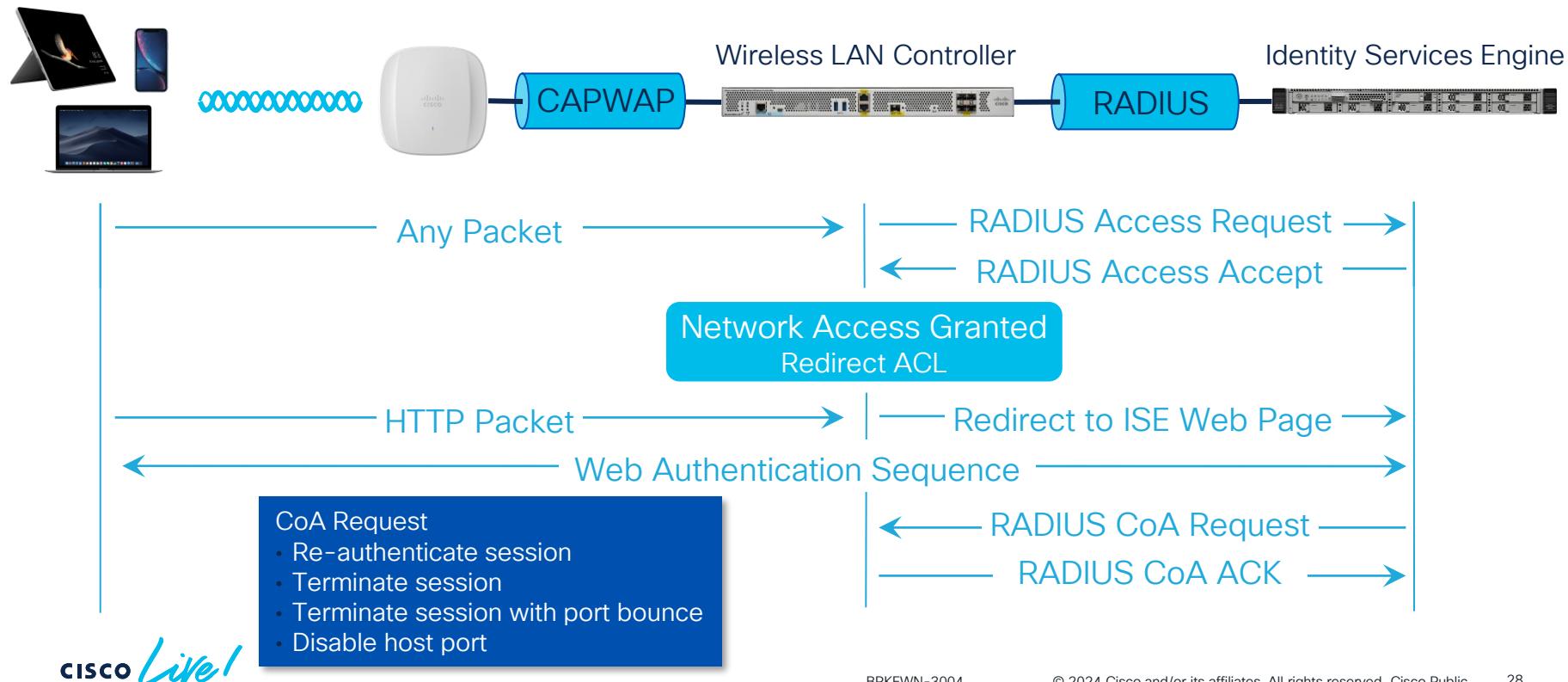
Cyber incident breakdown



- Ransomware
 - East/West Traversal
 - Authorisation
 - Micro-segmentation
 - Rapid Threat Containment
- Phishing and compromised or stolen credentials
 - Username/Password
 - Digital Certificates

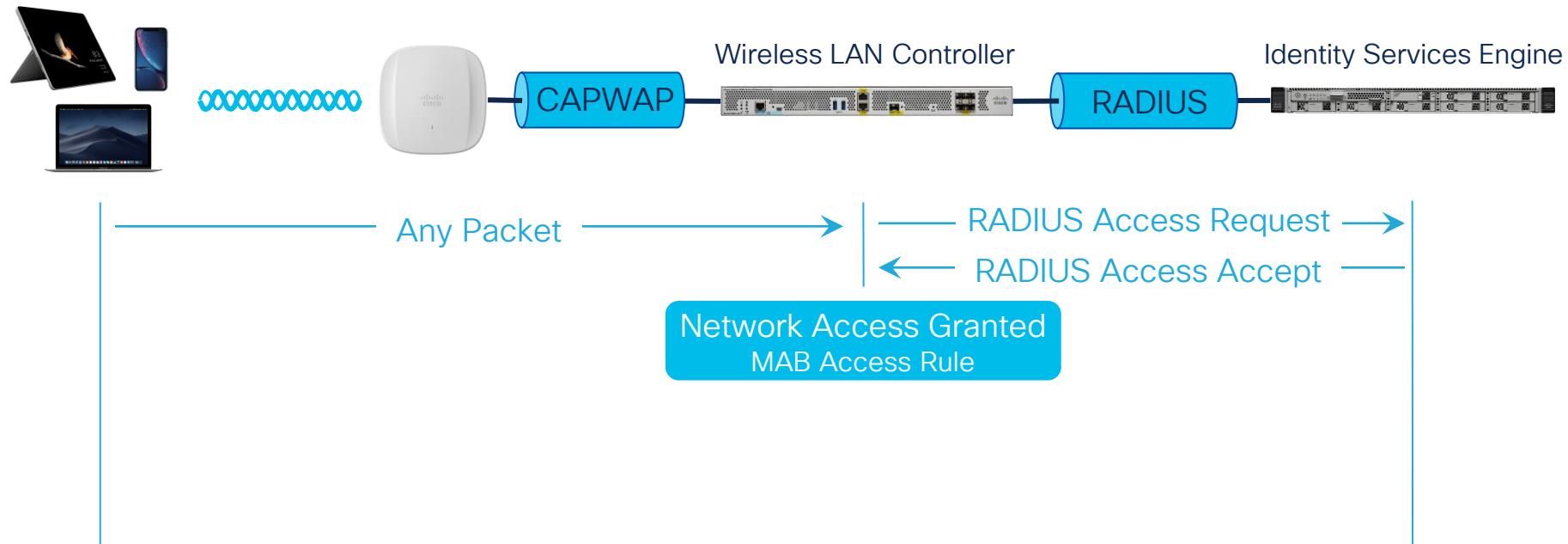
Central Web Authentication

URL Redirect



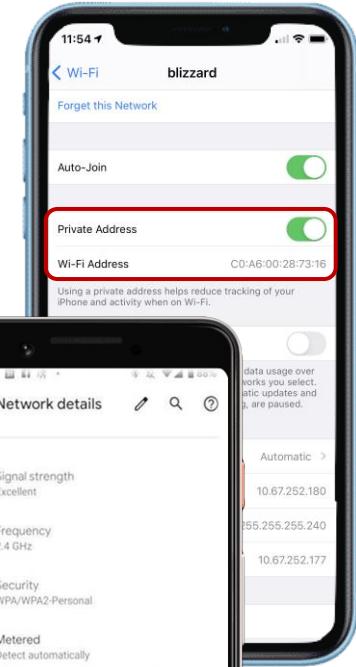
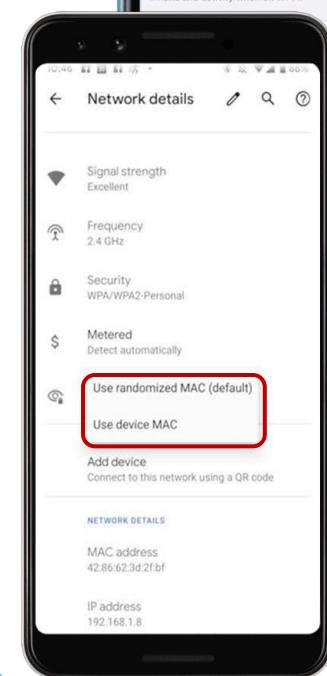
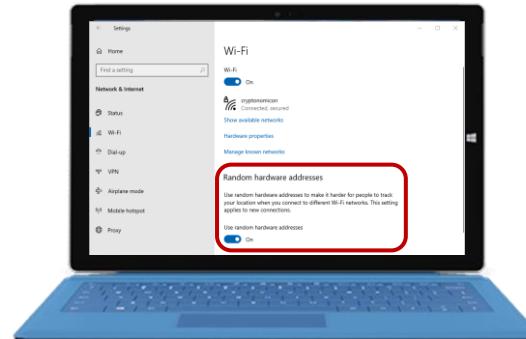
Central Web Authentication

MAC Authentication Bypass



Random MAC and Private Addresses

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



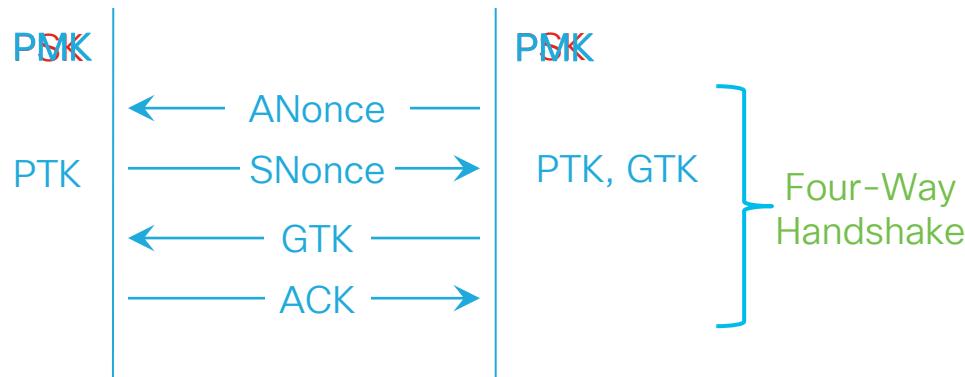
WPA Personal

Pre-Shared Key



WPA Personal

Pre-Shared Key



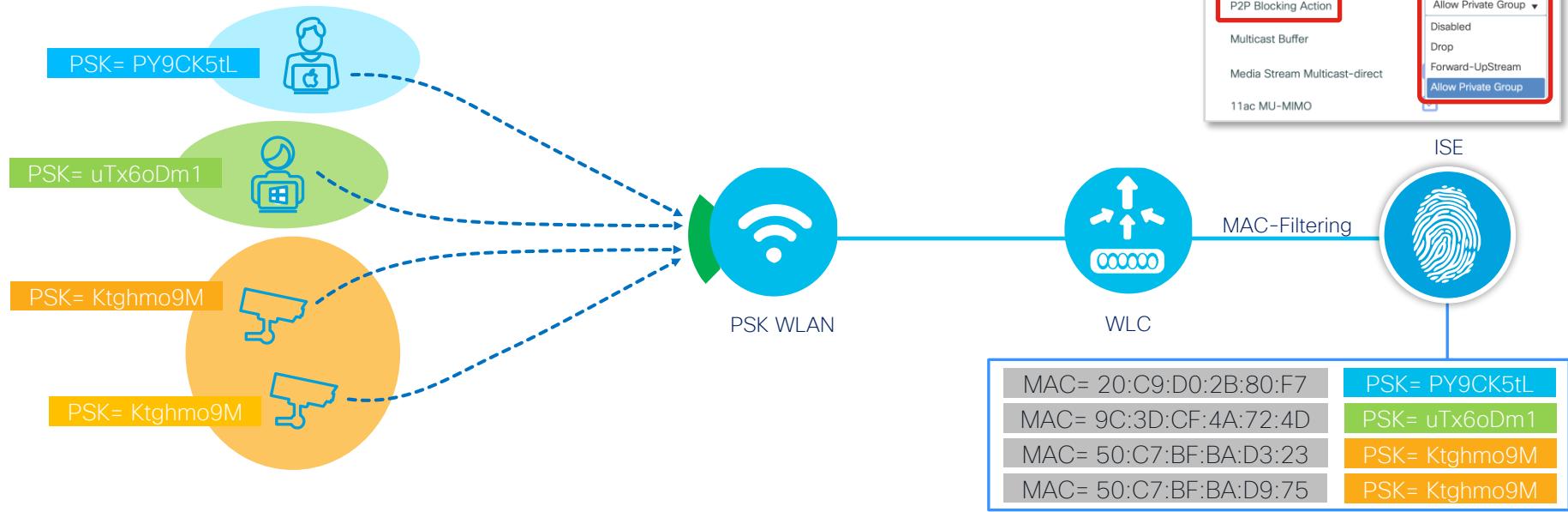
• Offline Attacks

- Dictionary
- Rainbow Table

• Strong Passwords Matter

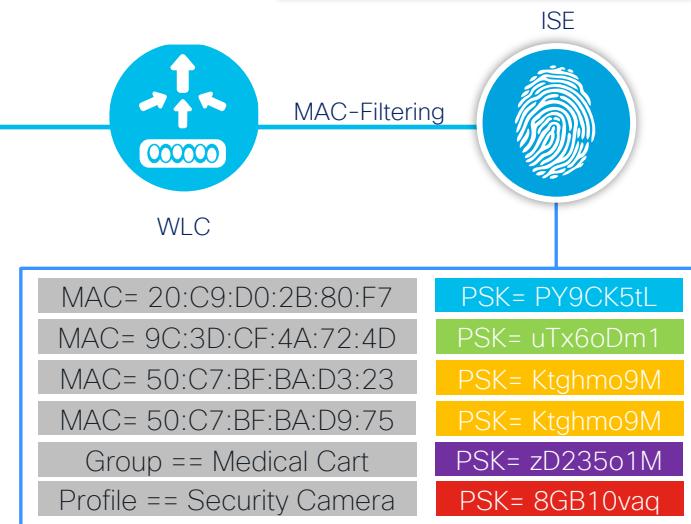
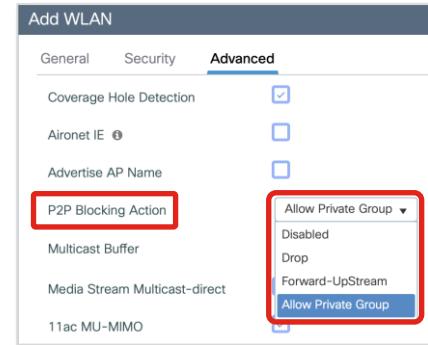
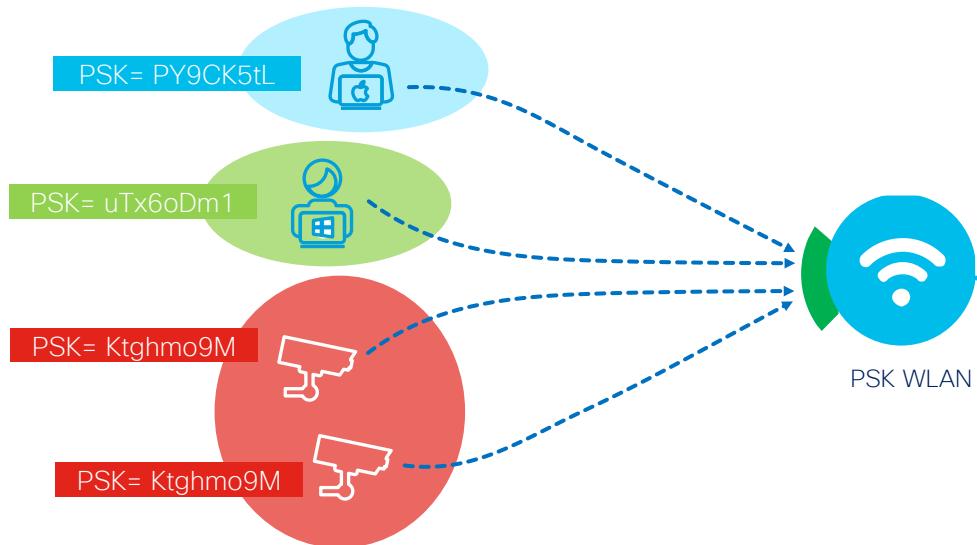
$$\text{PTK} = \text{SHA}(\text{PMK} + \text{ANonce} + \text{SNonce} + \text{AP MAC} + \text{STA MAC})$$

Identity PSK



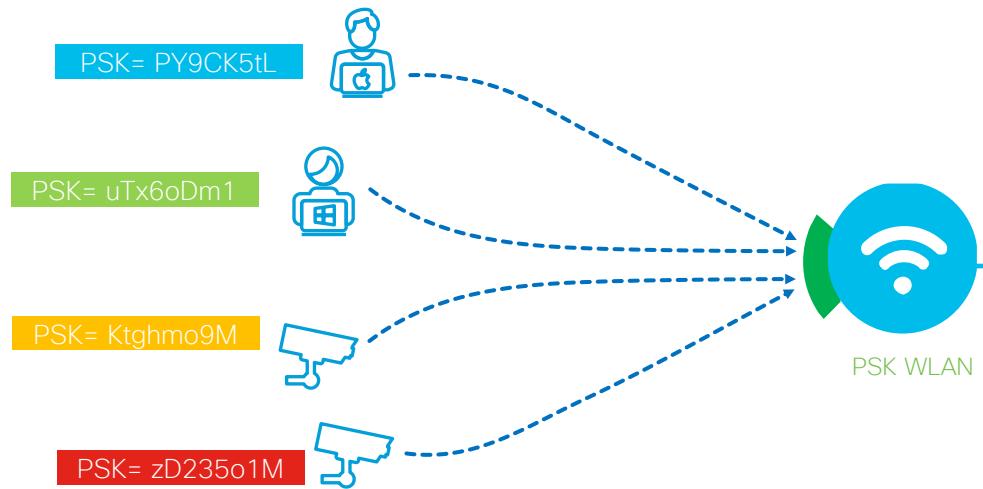
<https://www.cisco.com/c/en/us/support/docs/wireless/catalyst-9800-series-wireless-controllers/216130-configure-catalyst-9800-wlc-ipsk-with-ci.html>
https://documentation.meraki.com/MR/Encryption_and_Authentication/PSK_with_RADIUS_Authentication

Identity PSK

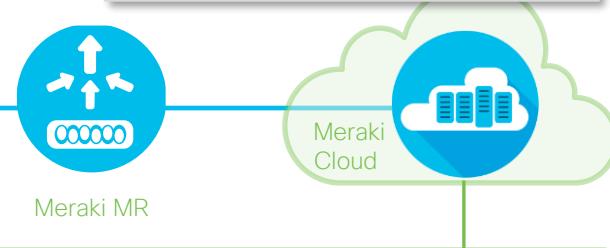


<https://www.cisco.com/c/en/us/support/docs/wireless/catalyst-9800-series-wireless-controllers/216130-configure-catalyst-9800-wlc-ipsk-with-ci.html>
https://documentation.meraki.com/MR/Encryption_and_Authentication/IPSK_with_RADIUS_Authentication

Identity PSK without RADIUS



Identity PSK without RADIUS		
Devices are assigned a group policy based on its passphrase		
Search Identity PSKs...		5001 Identity PSKs
Add	Delete	
<input type="checkbox"/>	Name	Pre-Shared Key
<input type="checkbox"/>	ipsk5
<input type="checkbox"/>	ipsk1
<input type="checkbox"/>	ipsk2
<input type="checkbox"/>	ipsk3
<input type="checkbox"/>	ipsk4



MAC = 20:C9:D0:2B:80:F7	PSK = PY9CK5tL
MAC = 9C:3D:CF:4A:72:4D	PSK = uTx6oDm1
MAC = 50:C7:BF:BA:D3:23	PSK = Ktghmo9M
MAC = 50:C7:BF:BA:D9:75	PSK = zD235o1M



Simultaneous Authentication of Equals

WPA3

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

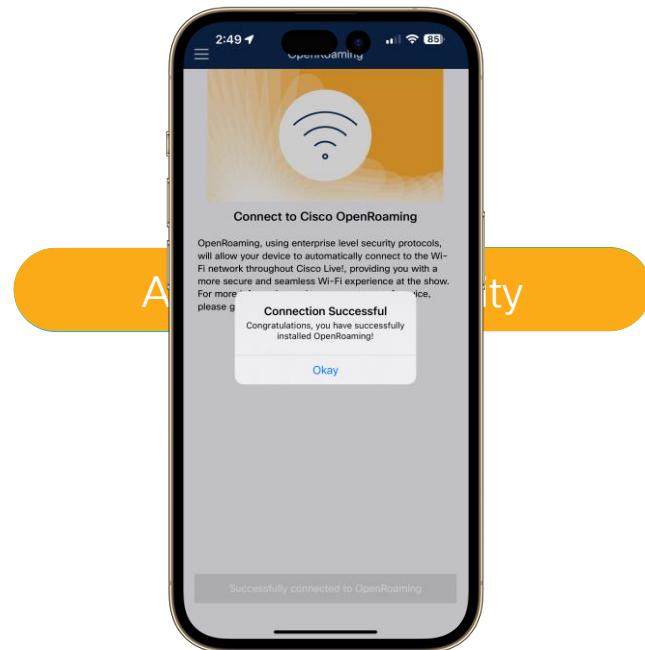


Wi-Fi Certified Enhanced Open

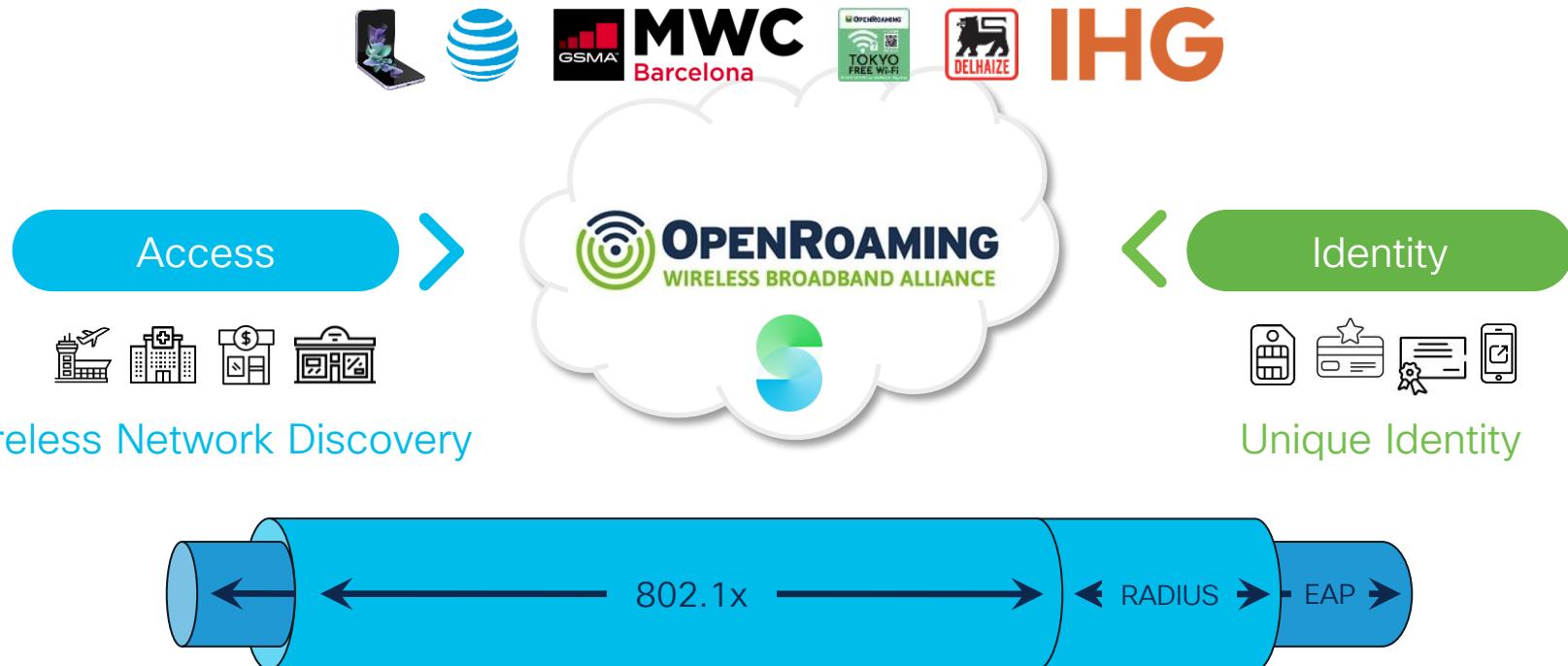
WPA3

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

Decoupling Access and Identity



OpenRoaming



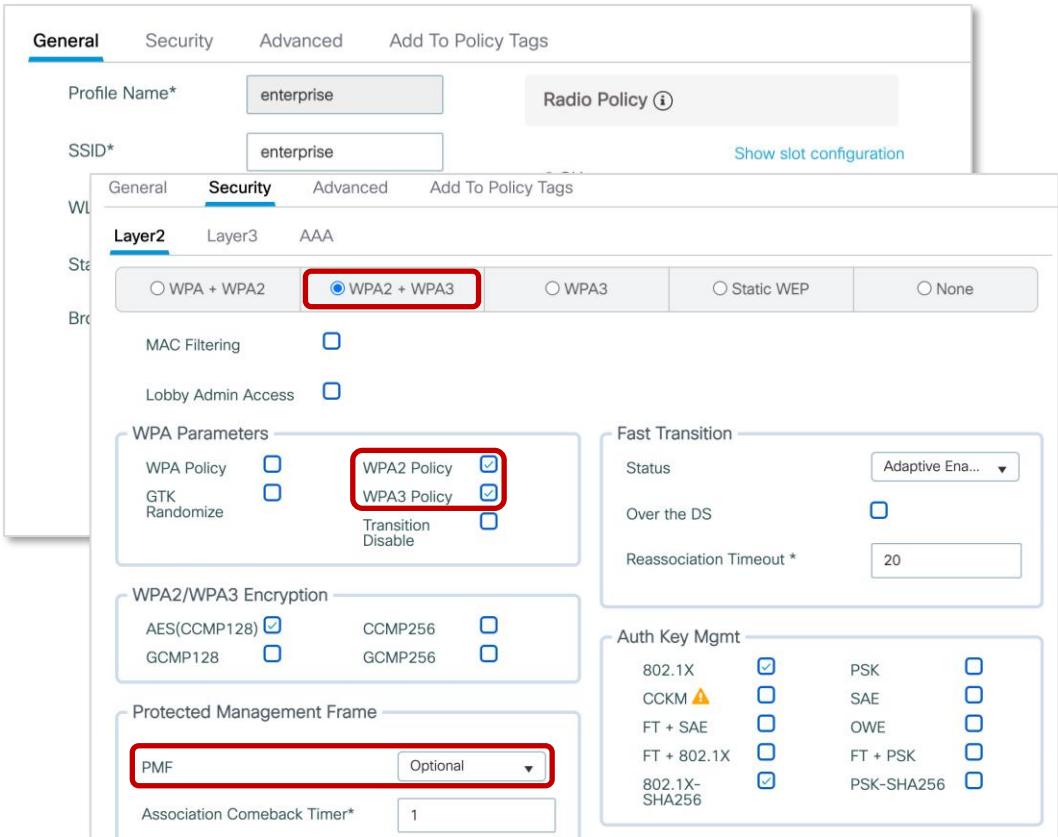
Implications of 6GHz



WPA3 and OWE are
mandatory for 6GHz



WPA2 and Open are not
supported on 6GHz



General Security Advanced Add To Policy Tags

Profile Name* enterprise Radio Policy ⓘ

SSID* enterprise Show slot configuration

General Security Advanced Add To Policy Tags

Layer2 Layer3 AAA

WPA + WPA2 WPA2 + WPA3 WPA3 Static WEP None

MAC Filtering

Lobby Admin Access

WPA Parameters

WPA Policy WPA2 Policy WPA3 Policy Transition Disable

GTK Randomize

Fast Transition

Adaptive Ena...

Over the DS

Reassociation Timeout* 20

WPA2/WPA3 Encryption

AES(CCMP128) CCMP256
GCMP128 GCMP256

Protected Management Frame

PMF Optional

Association Comeback Timer* 1

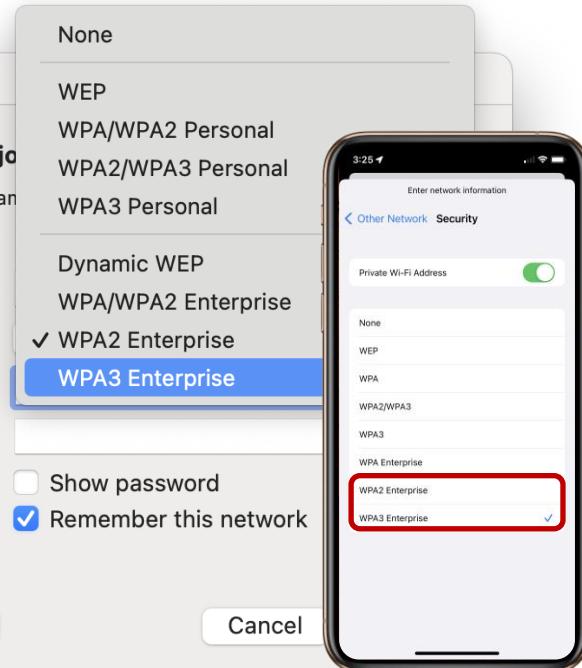
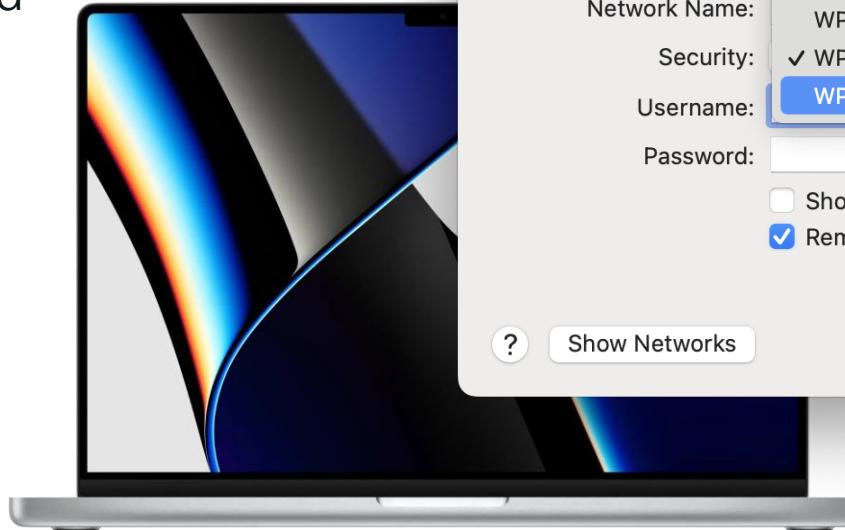
Auth Key Mgmt

802.1X PSK
CCKM ⚠ SAE
FT + SAE OWE
FT + 802.1X FT + PSK
802.1X-SHA256 PSK-SHA256



Wi-Fi 6E and Wi-Fi 7 Security

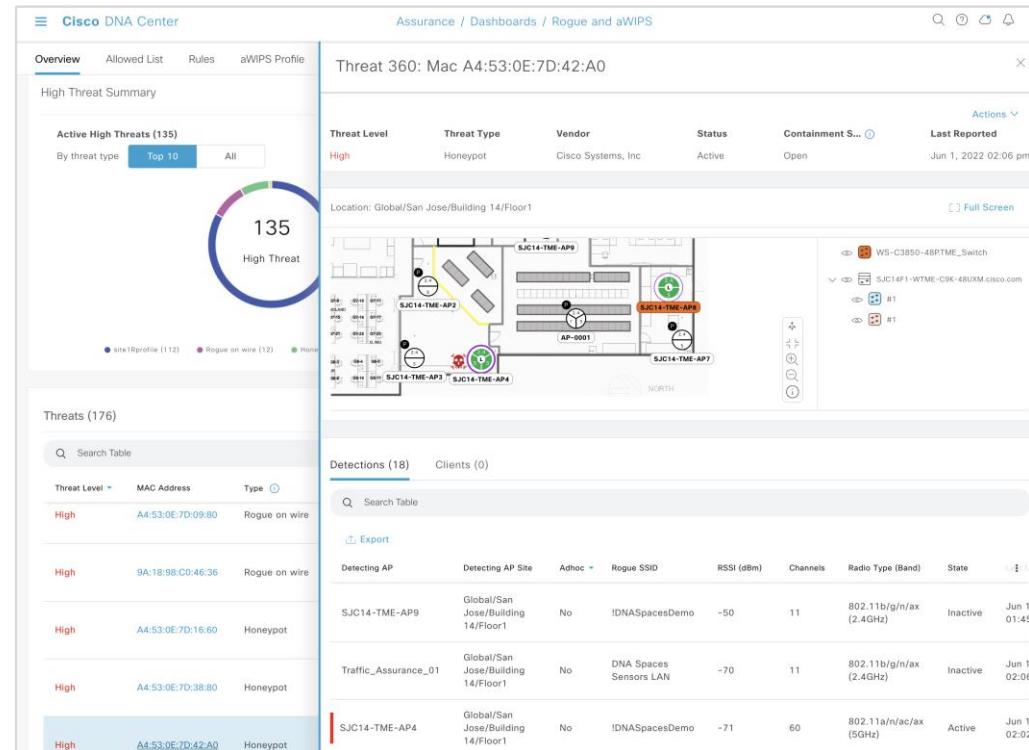
- Client device profiles must select WPA2 *or* WPA3
 - And only one profile for a given SSID is permitted



Rogue Detection and Advanced WIPS

Rogue Detection and Advanced WIPS

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



The image shows a screenshot of the Cisco DNA Center interface, specifically the 'Assurance / Dashboards / Rogue and aWIPS' section. The dashboard is titled 'Threat 360: Mac A4:53:0E:7D:42:A0'. It features several key components:

- High Threat Summary:** A circular chart showing '135 High Threat'.
- Threat Level:** A table showing Threat Level (High), Threat Type (HoneyPot), Vendor (Cisco Systems, Inc), Status (Active), and Containment Status (Open). Last Reported is Jun 1, 2022 02:06 pm.
- Location:** Global/San Jose/Building 14/Floor1. A map shows the building layout with various access points (AP-0001, SJC14-TME-AP9, SJC14-TME-AP2, SJC14-TME-AP3, SJC14-TME-AP4) and a highlighted rogue device.
- Threats (176):** A table listing threats by Threat Level (High), MAC Address, and Type (Rogue on wire, Rogue on air, HoneyPot). Examples include A4:53:0E:7D:09:80 (Rogue on wire), 9A:18:98:C0:46:36 (Rogue on wire), A4:53:0E:7D:16:60 (HoneyPot), A4:53:0E:7D:38:80 (HoneyPot), and A4:53:0E:7D:42:A0 (HoneyPot).
- Detections (18):** A table listing detections by Detecting AP, Detecting AP Site, Adhoc, Rogue SSID, RSSI (dBm), Channels, Radio Type (Band), and State. Examples include SJC14-TME-AP9 (Global/San Jose/Building 14/Floor1, Adhoc, !DNASpacesDemo, -50 dBm, 11 channels, 802.11b/g/n/ax (2.4GHz), Inactive), Traffic_Assurance_01 (Global/San Jose/Building 14/Floor1, Adhoc, DNA Spaces Sensors LAN, -70 dBm, 11 channels, 802.11b/g/n/ax (2.4GHz), Inactive), and SJC14-TME-AP4 (Global/San Jose/Building 14/Floor1, Adhoc, !DNASpacesDemo, -71 dBm, 60 channels, 802.11a/n/ac/ax (5GHz), Active).
- Clients (0):** A table showing 0 clients.

https://www.cisco.com/c/en/us/td/docs/cloud-systems-management/network-automation-and-management/dna-center-rogue-management-application/2-3-3/quick-start-guide/b_rogue_management_qsg_2_3_3.html

Rogue Detection and Advanced WIPS

- Wireless threat detection
- Forensic capture
- Client exclusion policies

Configuration > Security > Wireless Protection Policies

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

Select all events

Excessive 802.11 Association Failures

Excessive 802.1X Authentication Failures

Excessive 802.1X Authentication Timeout

IP Theft or IP Reuse

Excessive Web Authentication Failures

Captures (11)

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

aWIPS and Forensic Capture Enablement |

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

Enable aWIPS

Enable Forensic Capture (i)

Overview Threats Allowed List Rules aWIPS Profile

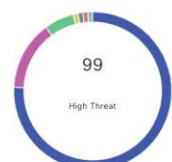
Site: Global May 7, 2022 8:26 PM - May 8, 2022 8:26 PM Last 24 hours Refresh Actions

	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



99

High Threat

Threat Type	Severity	Action		
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
Broadcast	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 Loc	RTS Flood	High	Predefined	Active
	RTS Virtual Carrier Sense Attack	High	Predefined	Active

Rogue Access Points

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

The image shows two screenshots of a network configuration interface. The top screenshot is titled 'Add AP Join Profile' and has a tab bar with 'General', 'Client', 'CAPWAP', 'AP', 'Management', 'Security' (which is underlined in blue), 'ICap', and 'QoS'. Below this is a section titled 'Rogues' with a checkbox labeled 'Rogue Detection' which is checked. There are also fields for 'Rogue Detection Minimum RSSI' (set to -90) and 'Rogue Detection Transient Interval (seconds)' (set to 0). The bottom screenshot is titled 'Configuration > Security > Wireless Protection Policies' and shows a tab bar with 'Rogue Policies' (which is underlined in red), 'Rogue AP Rules' (which is highlighted with a red box), and 'Client Exclusion Policies'. The 'Rogue Policies' tab is active and displays various configuration options. One of these options, 'Auto Contain' with the sub-option 'Using our SSID' (also highlighted with a red box), is selected. Other options include 'Auto Containment only for Monitor Mode APs' (unchecked), 'Valid client on Rogue AP' (unchecked), and 'Adhoc Rogue AP' (unchecked). The 'MFP Configuration' section includes 'Global MFP State' (unchecked), 'AP Impersonation Detection' (unchecked), and 'MFP Key Refresh Interval (hours)' (set to 24). The 'Rogue Policies' section includes fields for 'Rogue Detection Security Level' (set to 'Custom'), 'Expiration timeout for Rogue APs (seconds)*' (set to 1200), 'Validate Rogue Clients against AAA' (unchecked), 'Validate Rogue APs against AAA' (unchecked), 'Rogue Polling Interval (seconds)' (set to 3600), 'Detect and Report Adhoc Networks' (checked), 'Rogue Detection Client Number Threshold*' (set to 0), 'Rogue Init Timer (seconds)*' (set to 180), 'AP Authentication' (unchecked), 'AP Authentication Alarm Threshold*' (set to 1), and 'Syslog Notification' (unchecked).

Rogue Clients

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

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

Configuration > Security > Wireless Protection Policies

Rogue Policies Rogue AP Rules Client Exclusion Policies

General

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

Auto Contain

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

MFP Configuration

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

Apply

Cisco Catalyst Centre Threat Levels

Informational

- RSSI <= -75 dBm and not on wire
- Rogue Type: Neighbor

Potential

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

High

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

Rogue AP Containment

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

The screenshot displays the Cisco DNA Center interface for 'Rogue and aWIPS' threats. At the top, a banner for 'Threat 360: Mac A4:53:0E:7C:99:E0' is shown, indicating a 'High Threat' level. Below this, a 'Warning' message states: '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 proceed?'. The main table lists two threats: 'Threat 360: Mac C6:9E:38:75:52:D8' (Potential, Interferer, UNKNOWN, Active, Open) and 'Threat 360: Mac A4:53:0E:7C:99:E0' (High, Honeypot, Cisco Systems, Inc., Active, Open). The bottom section shows a network map of 'SJC14-TME' with four access points (AP-0001, AP-0002, AP-0003, AP-0004) and various floor plans. A red circle highlights a specific location on the map, and a yellow line connects it to the threat details above.

Rogue Containment with WPA3

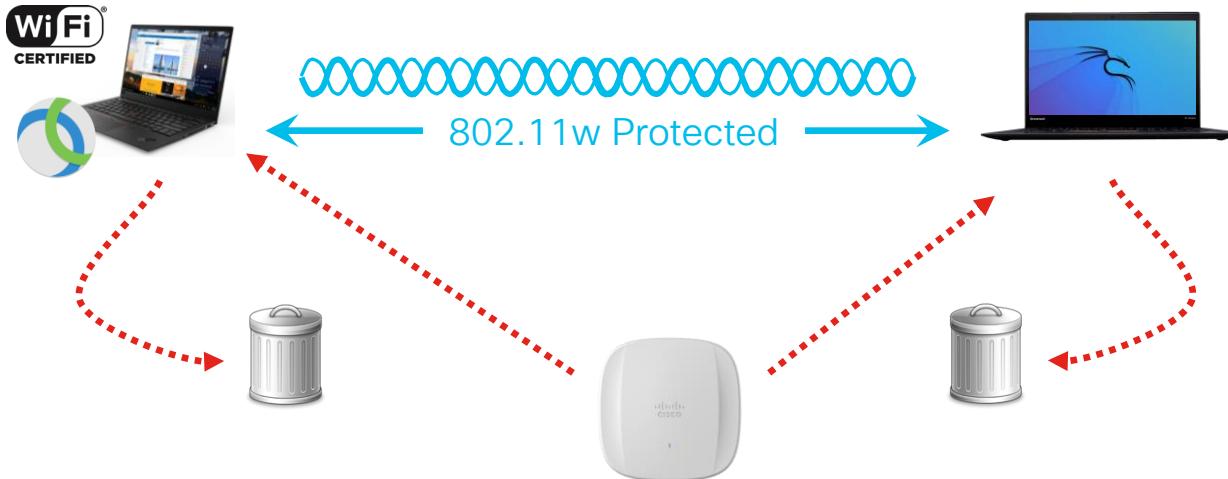
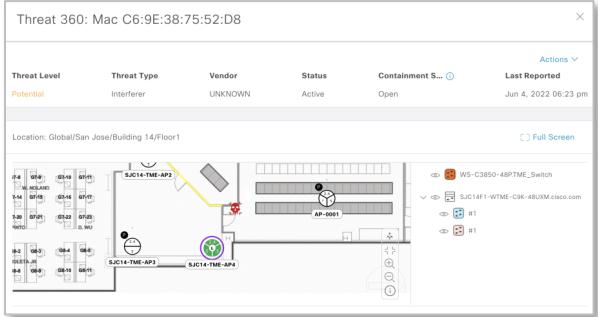
Threat 360: Mac C6:9E:38:75:52:D8

Actions

Threat Level	Threat Type	Vendor	Status	Containment S...	Last Reported
Potential	Interferer	UNKNOWN	Active	Open	Jun 4, 2022 06:23 pm

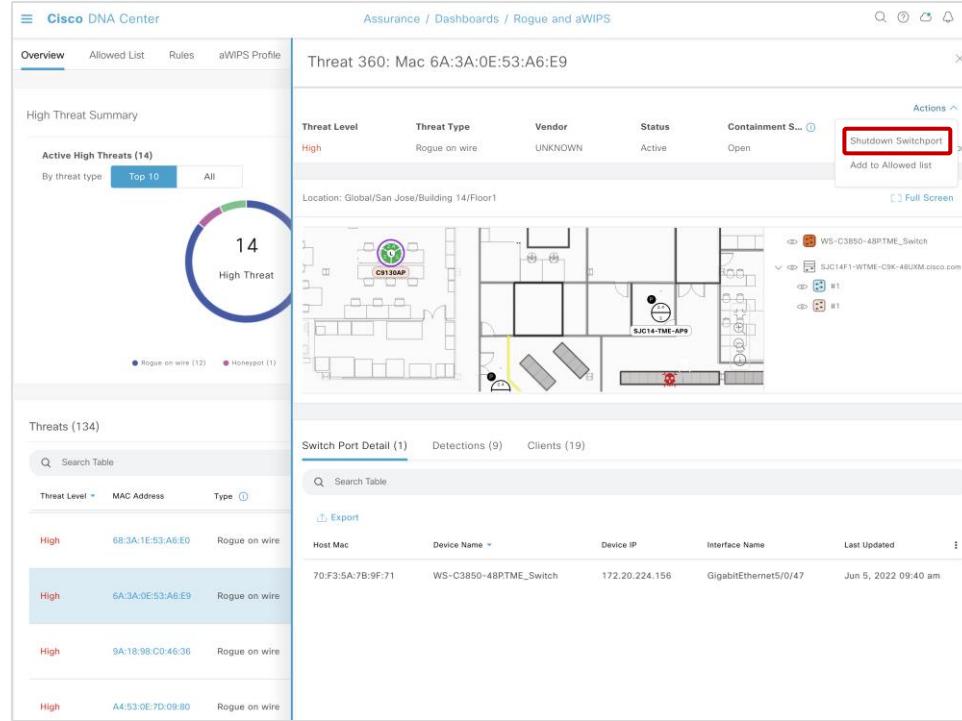
Location: Global/San Jose/Building 14/Floor 1

Full Screen



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 shows the Cisco DNA Center interface for managing rogue and aWIPS threats. The main dashboard displays a 'High Threat Summary' with 14 active high threats, categorized as 'Rogue on wire' (12) and 'Honeypot' (1). A detailed threat card for 'Threat 360: Mac 6A:3A:0E:53:A6:E9' is shown, with options to 'Shutdown Switchport' or 'Add to Allowed list'. The dashboard also includes a floor plan showing the location of the rogue AP (SJC14-TME-AP9) and a table of switch port details, detections, and clients.

High Threat Summary

Active High Threats (14)

Threat Level: High, Threat Type: Rogue on wire, Vendor: UNKNOWN, Status: Active, Containment State: Open

Location: Global/San Jose/Building 14/Floor 1

Switch Port Detail (1)

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

Air Marshal

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

Air Marshal

Configure Rogue SSIDs 24 Other SSIDs 595 Spoofs 31 Malicious broadcasts 0 Packet floods 0

24 rogue SSIDs seen for the last 2 hours

SSID	Broadcast MACs	Last seen	First seen	Containment	Rogue because
AXE BLE testing (and 1 other)	6:e:3a:0e:ff:f8:f5	4 seconds ago	1 year ago	partial	Recently seen on LAN
IT Test WiFi	e:0:cb:bc:49:35:61 (and 1 other)	50 seconds ago	1 month ago	contained	Recently seen on LAN
j-bond-2-owe	c:6:14:92:6:e:ae:b2 (and 2 others)	15 seconds ago	2 months ago	partial	Recently seen on LAN
j-bond-3-sae	ca:14:a2:6:e:ae:b0 (and 1 other)	15 seconds ago	3 weeks ago	partial	Recently seen on LAN
j-bond-5-1x	c:6:14:92:6:e:ae:a5 (and 4 others)	6 seconds ago	3 weeks ago	partial	Recently seen on LAN
j-bond-8-owe-8	c:6:14:92:6:e:ae:b8 (and 2 others)	7 seconds ago	3 weeks ago	partial	Recently seen on LAN
j-p1-bond-2-owe	c:6:14:92:6:e:ae:a2 (and 4 others)	57 seconds ago	3 weeks ago	partial	Recently seen on LAN
j-p1-bond-3-sae	c:6:14:92:6:e:ae:a3 (and 4 others)	57 seconds ago	3 weeks ago	partial	Recently seen on LAN
j-p1-bond-4-sae	c:6:14:92:6:e:ae:b4 (and 5 others)	12 seconds ago	22 hours ago	partial	Recently seen on LAN
Meraki Setup	0:0:18:0a:36:d9:3e (and 98 others)	a moment ago	1 year ago	partial	Recently seen on LAN

10 results per page

Map view: Mission Bay Boulevard South, Bridgeway Way, Terry Francois Blvd. (Google Map data ©2023 Google)

SSID: IT Test WiFi edit
Containment: contained
Last seen: Wednesday 11/29/2023 8:25 pm
First seen: Wednesday 10/18/2023 7:18 am
1 month ago
Channels: 1, 149
VLANs: 0
Broadcast MACs: e:0:cb:bc:49:35:61 edit
e:2:cb:ac:49:35:61 edit
Wired MACs: e:0: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

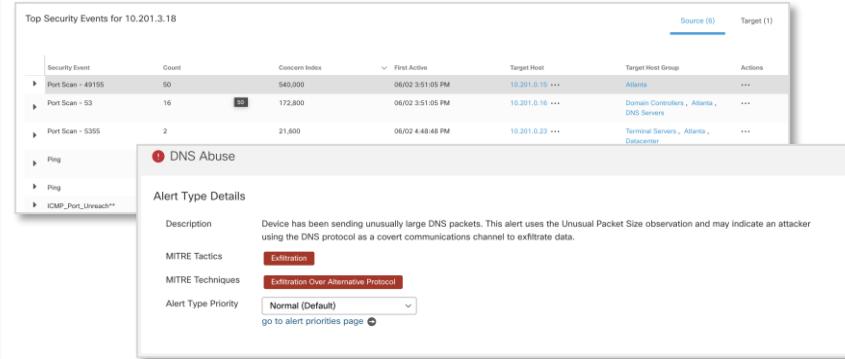
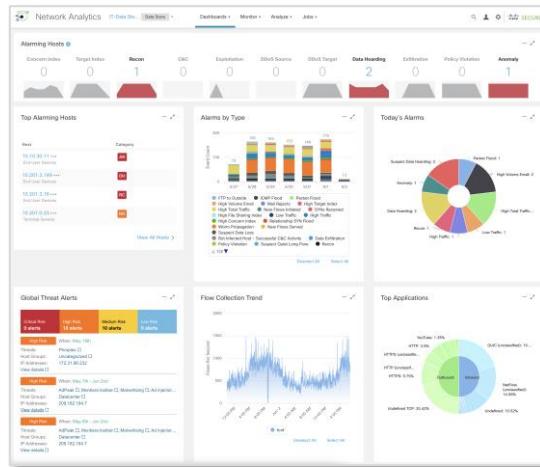
Secure Network Analytics Integration



Netflow

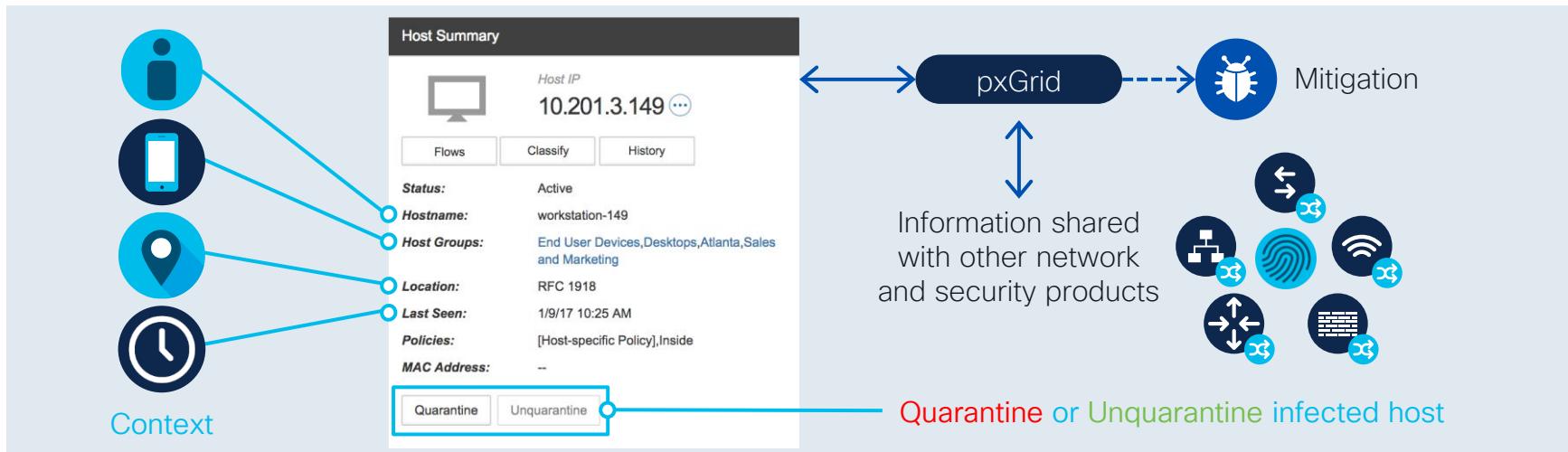


Malware detection and cryptographic compliance on Cisco Stealthwatch



Network as an Enforcer

Rapid Threat Containment



Securing the Wireless Network



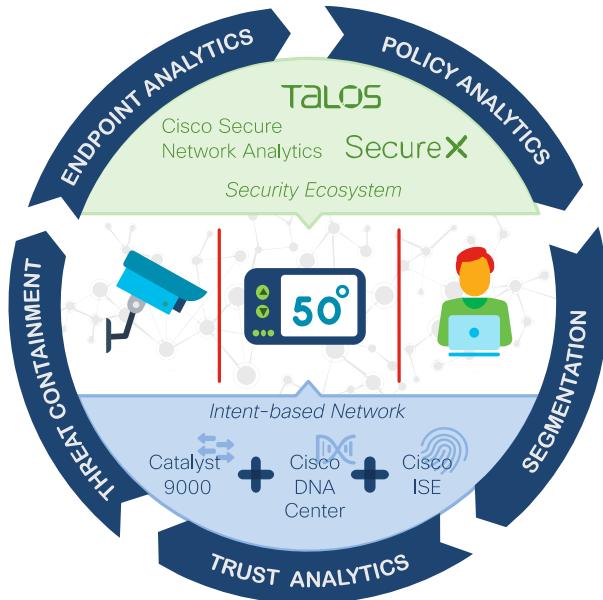
Secure the Air



Secure the Devices



Secure the Network





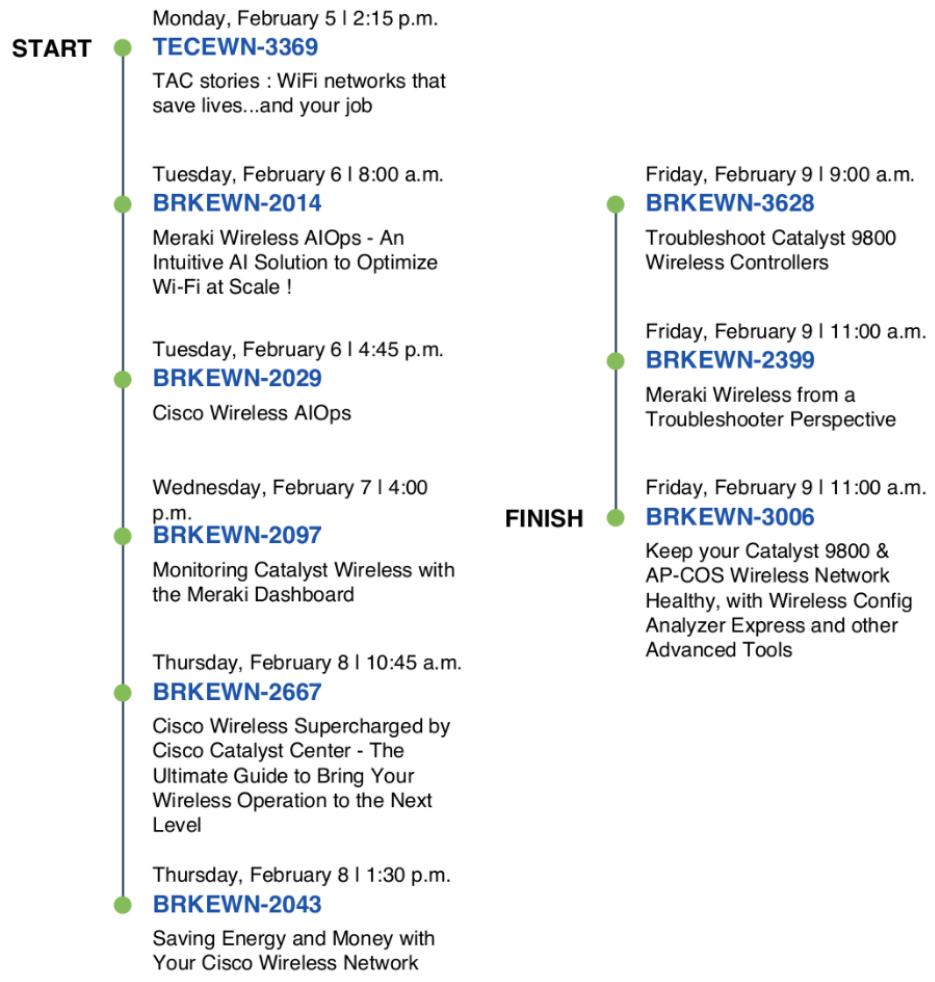
The bridge to possible

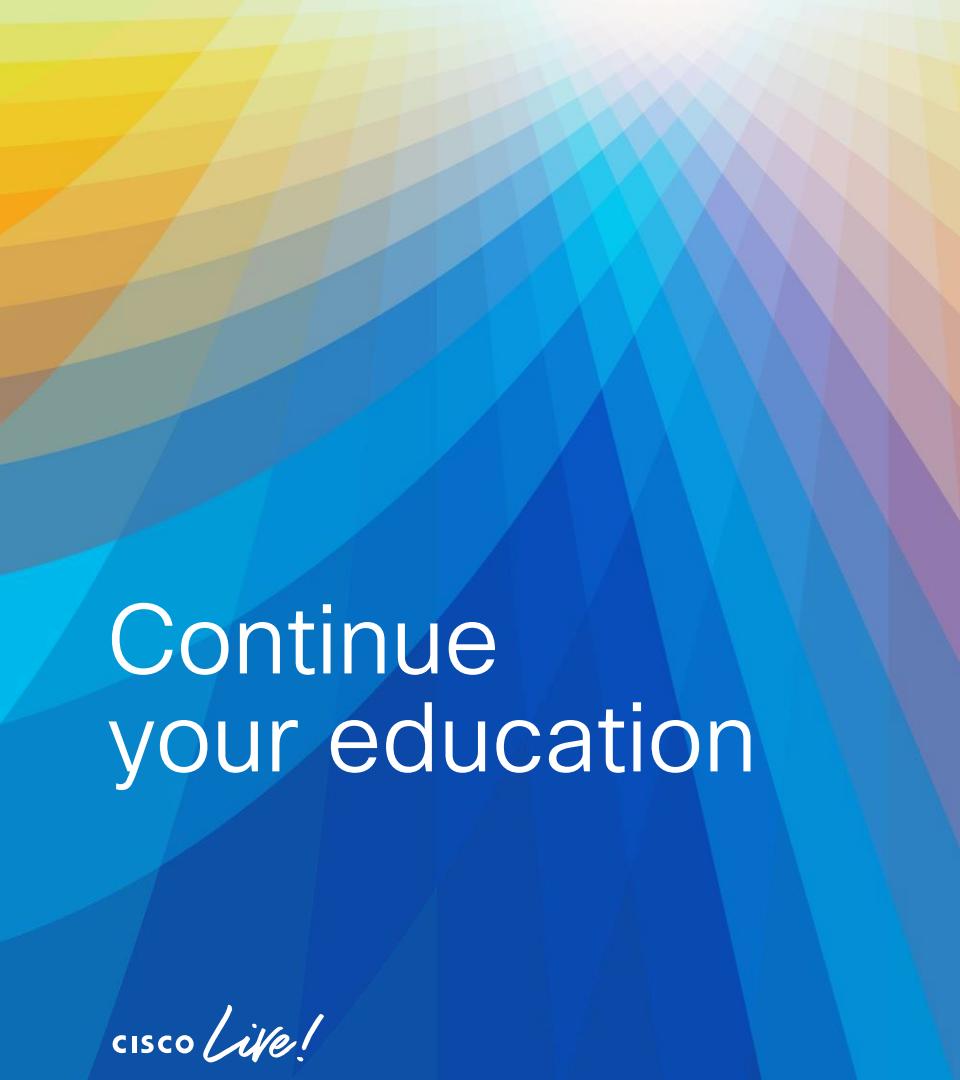
Thank you

CISCO Live!

Continue your education

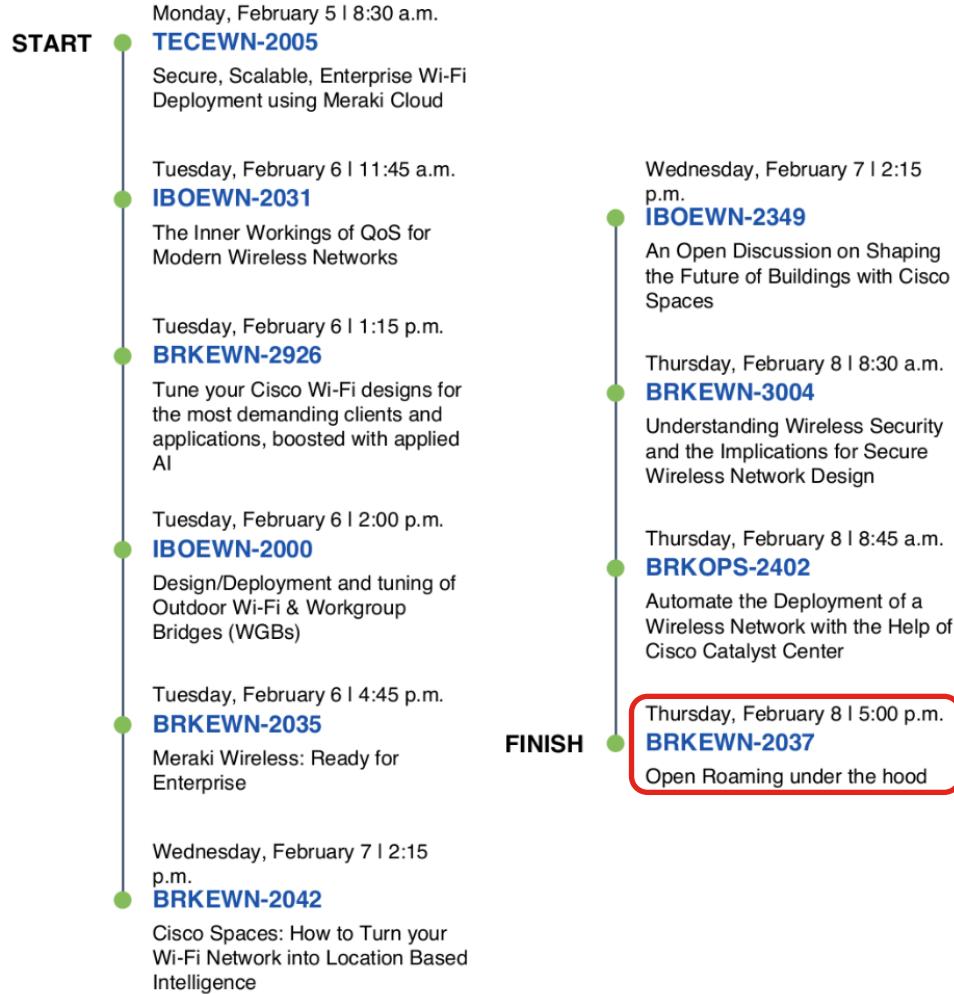
CISCO Live!





Continue your education

CISCO Live!



cisco *Live!*

Let's go