
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

cisco Live!

BRKEWN-3004

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

cisco Live!

Securing the Wireless Network

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

Tal Arad, CISO and Head of Technology, Carlsberg

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

Wireless Attack Surface

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

Wireless Protected Access

WPA	• A snapshot of the 802.11i Wireless Security Standard • Commonly used with TKIP encryption
WPA2	• Final version of 802.11i Wireless Security Standard • Commonly used with AES encryption
Authentication Mechanisms	• Personal (PSK – Pre-Shared Key) • Enterprise (802.1X/EAP)
WPA3	• Wi-Fi Alliance security update • Includes new capabilities and new certification requirements

WPA3

- Mandatory for Wi-Fi 6 Certification
- Remove insecure legacy protocols
  - WEP
  - TKIP
  - SHA1
- Negative Testing
  - KRACK

- Protected Management Frames (802.11w)
- Simultaneous Authentication of Equals (SAE)

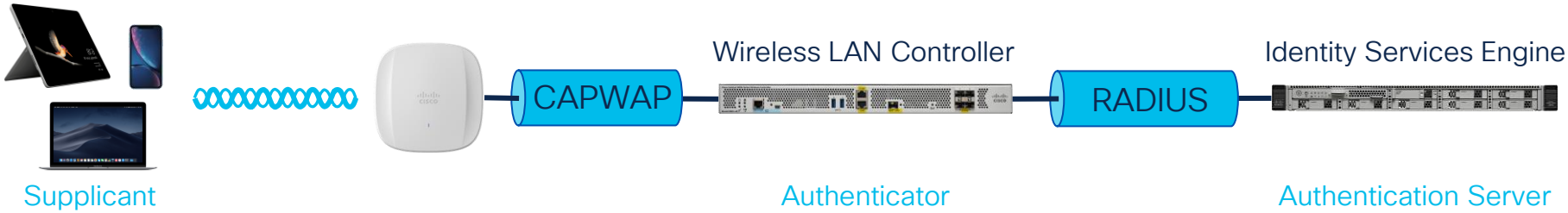
- Wi-Fi Certified Enhanced Open
  - Opportunistic Wireless Encryption (OWE)

802.11 Fundamentals

Authentication

802.11 Fundamentals

Authentication

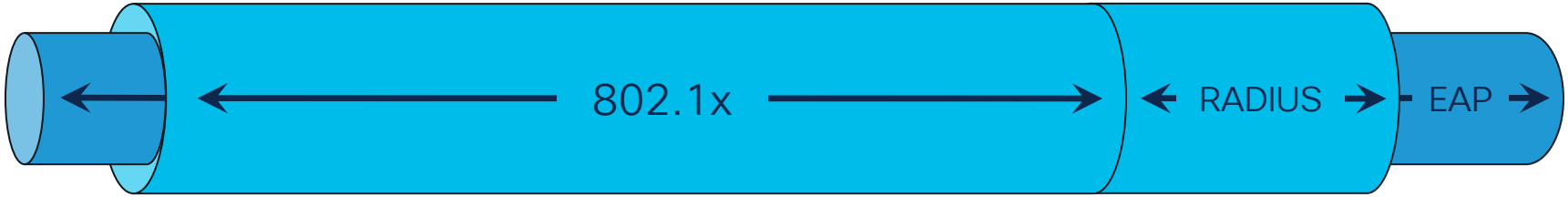


802.11 Fundamentals

Authentication

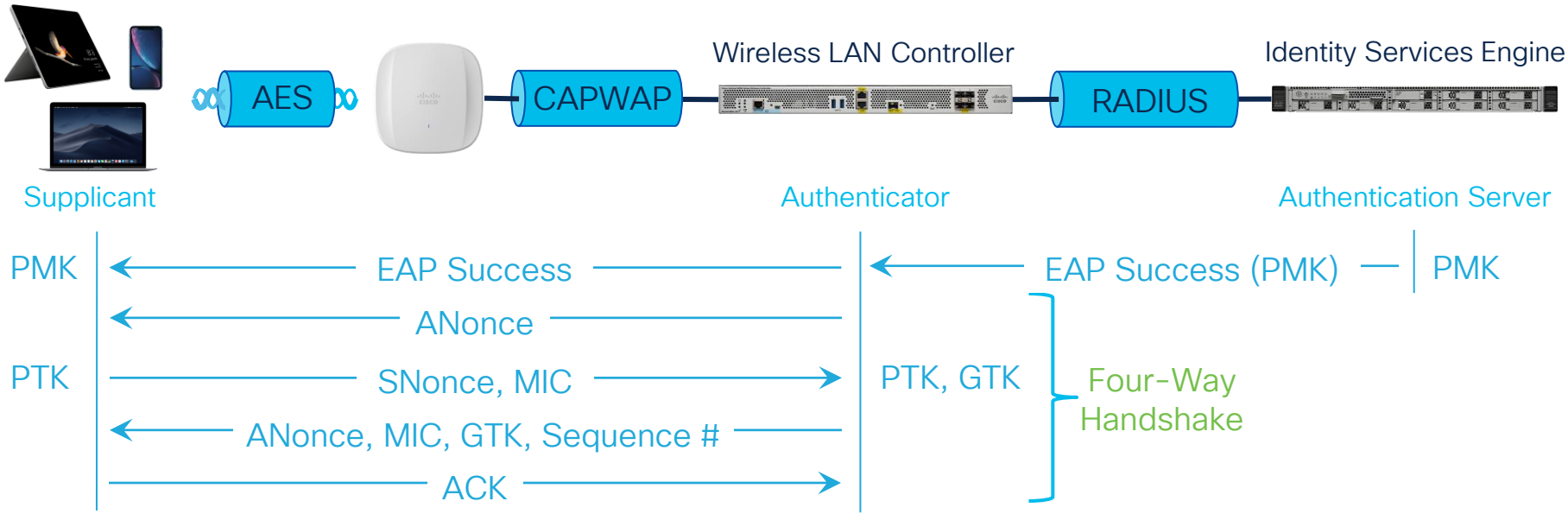
802.11 Fundamentals

Authentication



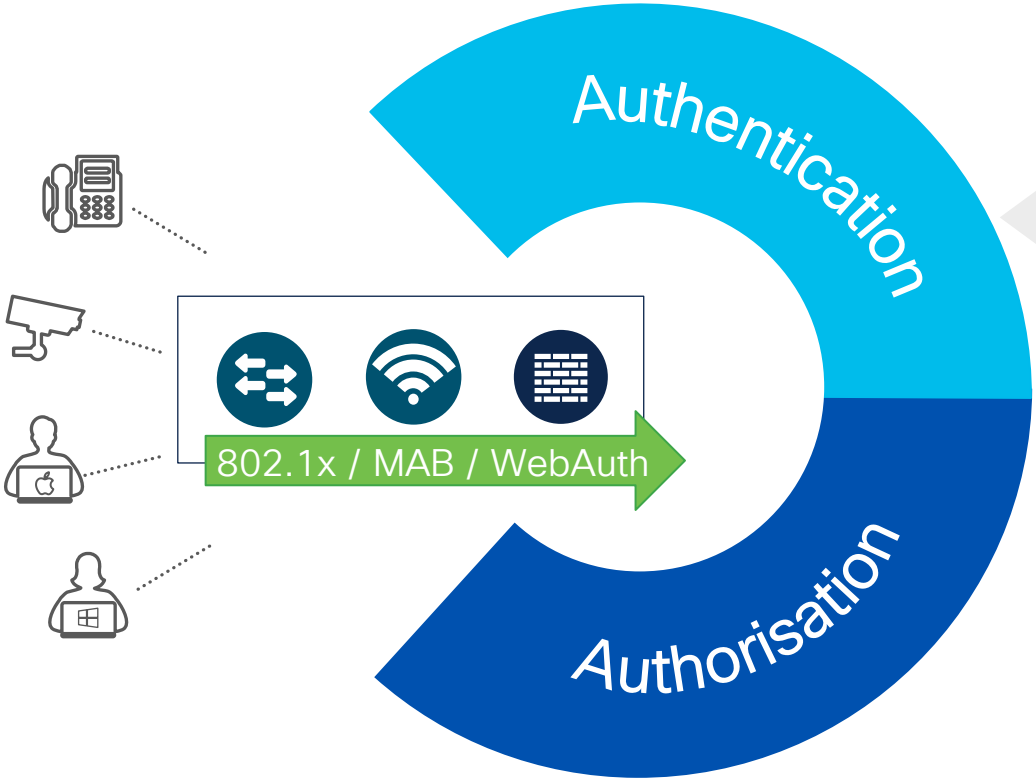
802.11 Fundamentals

Encryption



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

Authentication and Authorisation



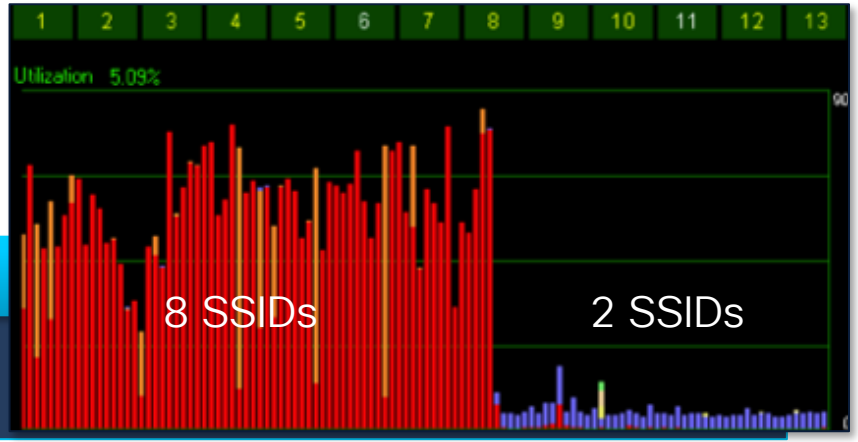
- Device Posture
- Device Type
- User Credentials
- MAC Address
- **Identity Elements**

- Location
- Day and Time
- Access Type
- Context

- **Policy Elements**
- VLAN/VN
- SGT / Group Policy
- QoS / BDRL
- URL Redirect / Filter
- Bonjour Service Policy
- Application Control

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

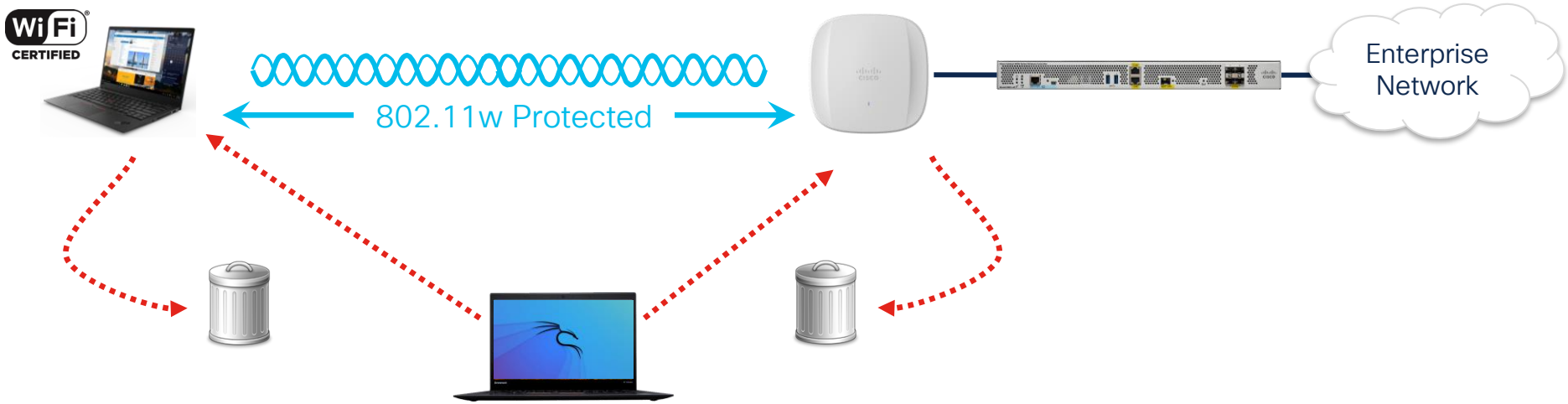
- Client channel scanning and AP selection
  - 802.11k Neighbor Lists based on CCX (Cisco Compatible Extensions)
  - 802.11v BSS Transition
- Re-authentication of client device and re-keying
  - 802.11r Fast BSS Transition based on CCKM (Cisco Centralised Key Management)

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

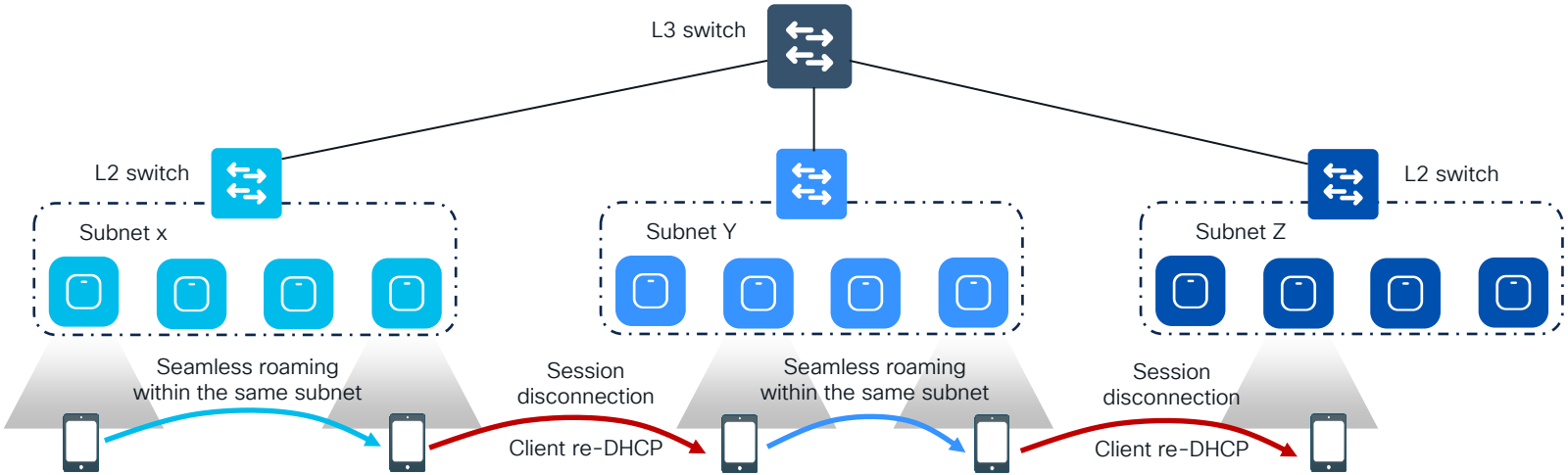
802.11w Protected Management Frames



Seamless Roaming at Scale

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

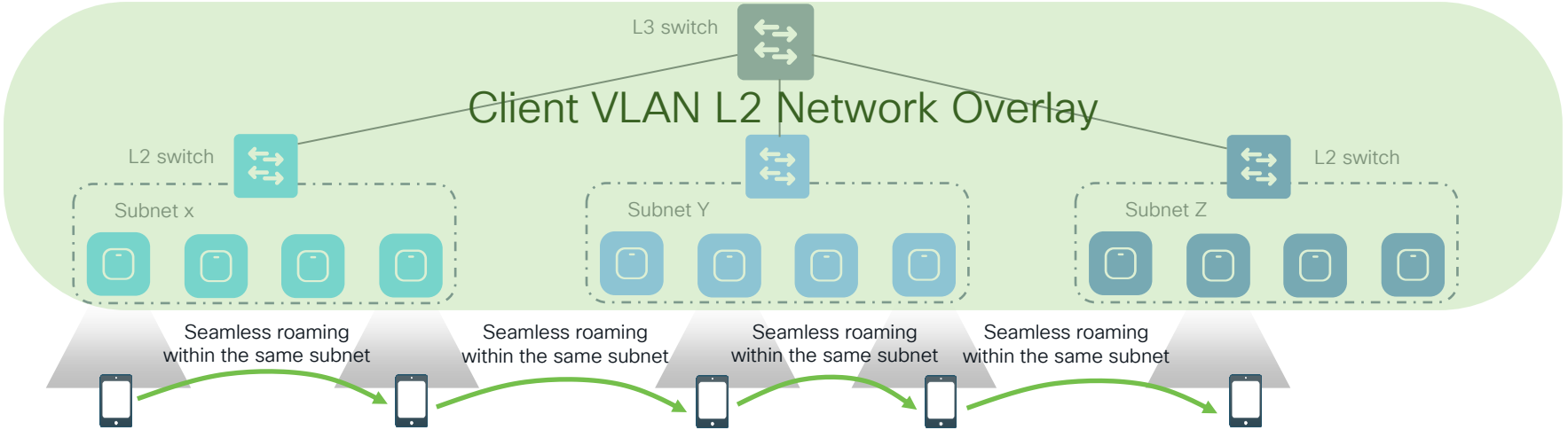
Large broadcast domains do not scale and is counter to networking best practice



Seamless Roaming at Scale

For L3 seamless roaming an extended VLAN network overlay is required

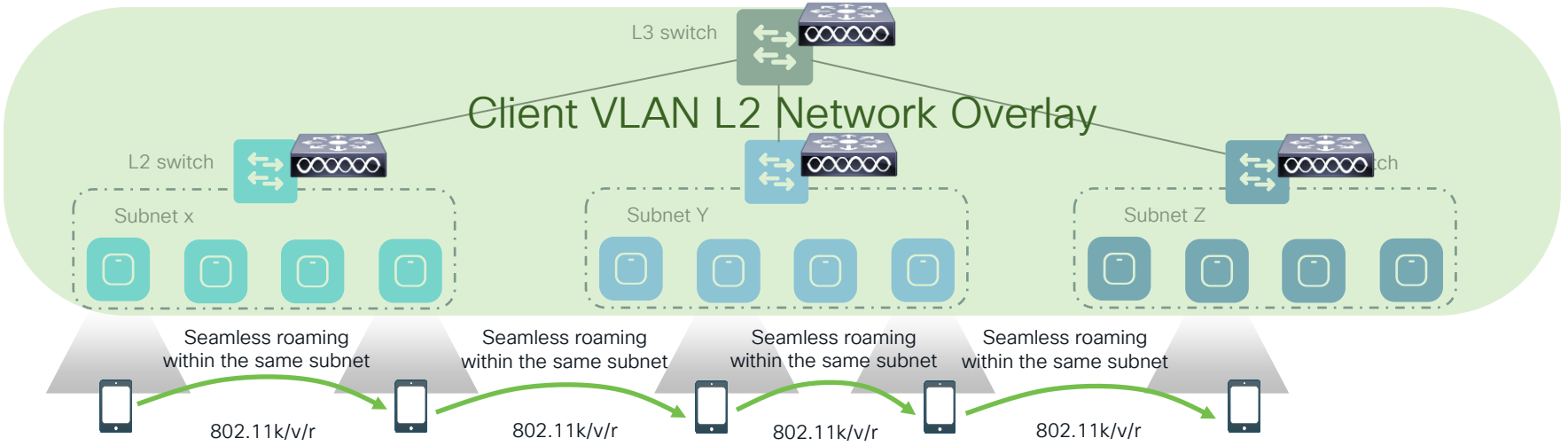
A data termination point is required to roam across L3 boundaries



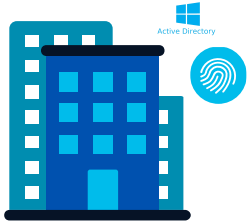
Seamless Roaming at Scale

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

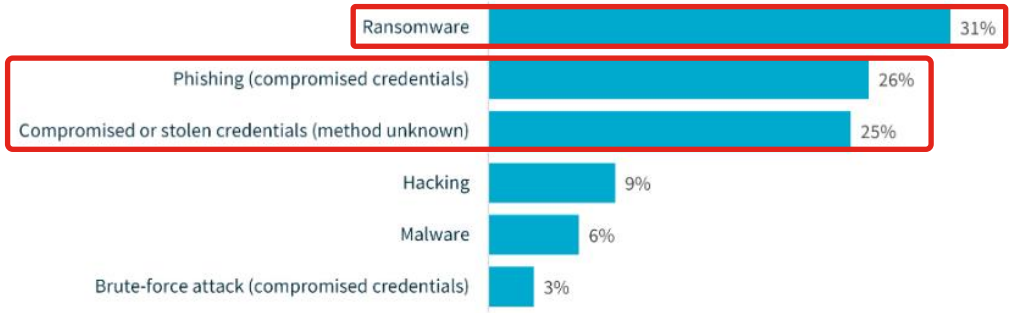
Cloud Identity with EAP-TLS

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

Any Packet

RADIUS Access Request

RADIUS Access Accept

Network Access Granted
Redirect ACL

HTTP Packet

Redirect to ISE Web Page

Web Authentication Sequence

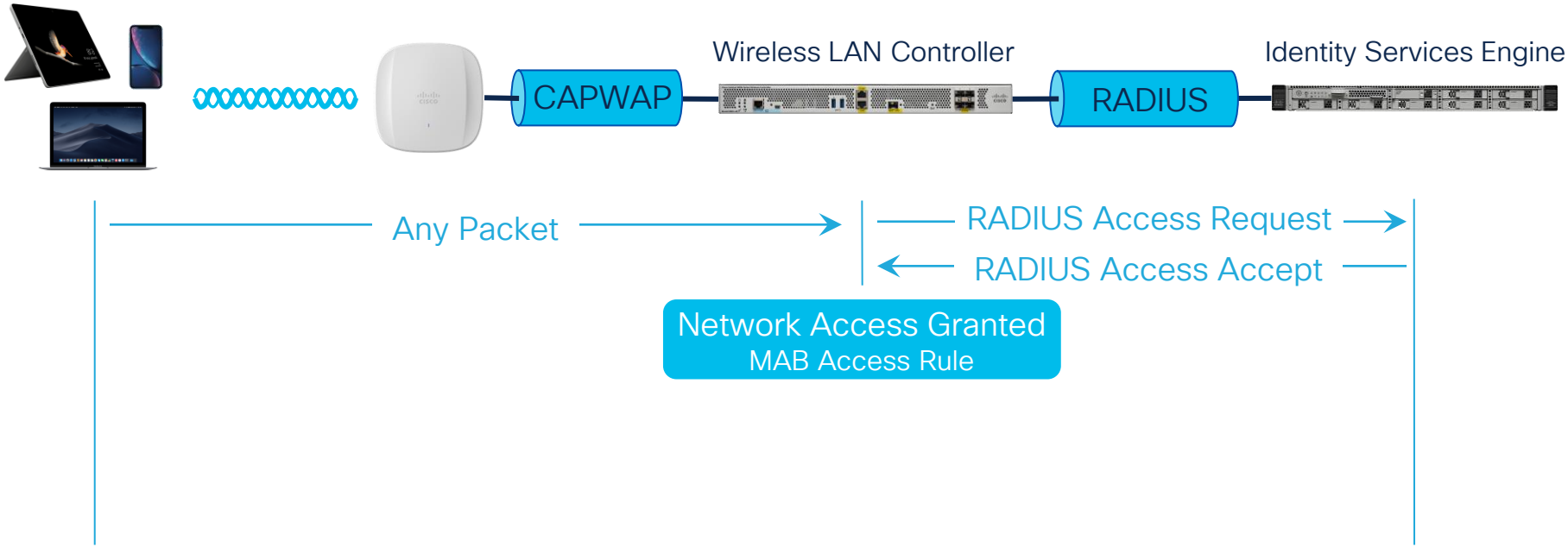
CoA Request
- Re-authenticate session
- Terminate session
- Terminate session with port bounce
- Disable host port

RADIUS CoA Request

RADIUS CoA ACK

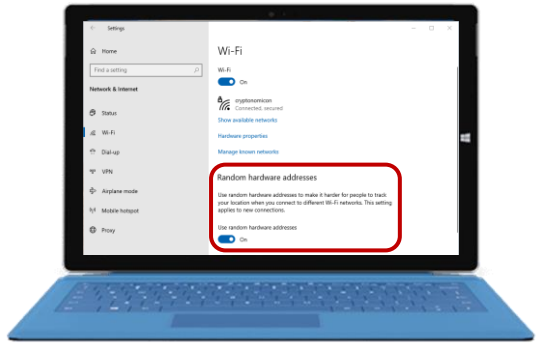
Central Web Authentication

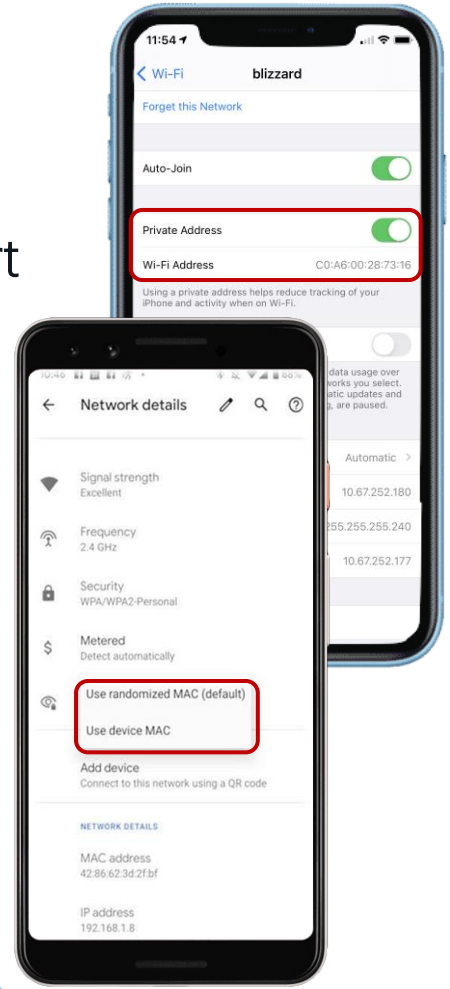
MAC Authentication Bypass



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



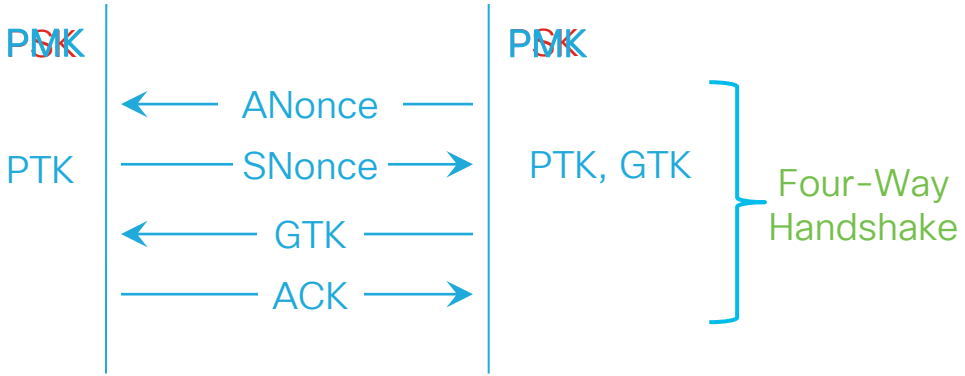


WPA Personal

Pre-Shared Key

WPA Personal

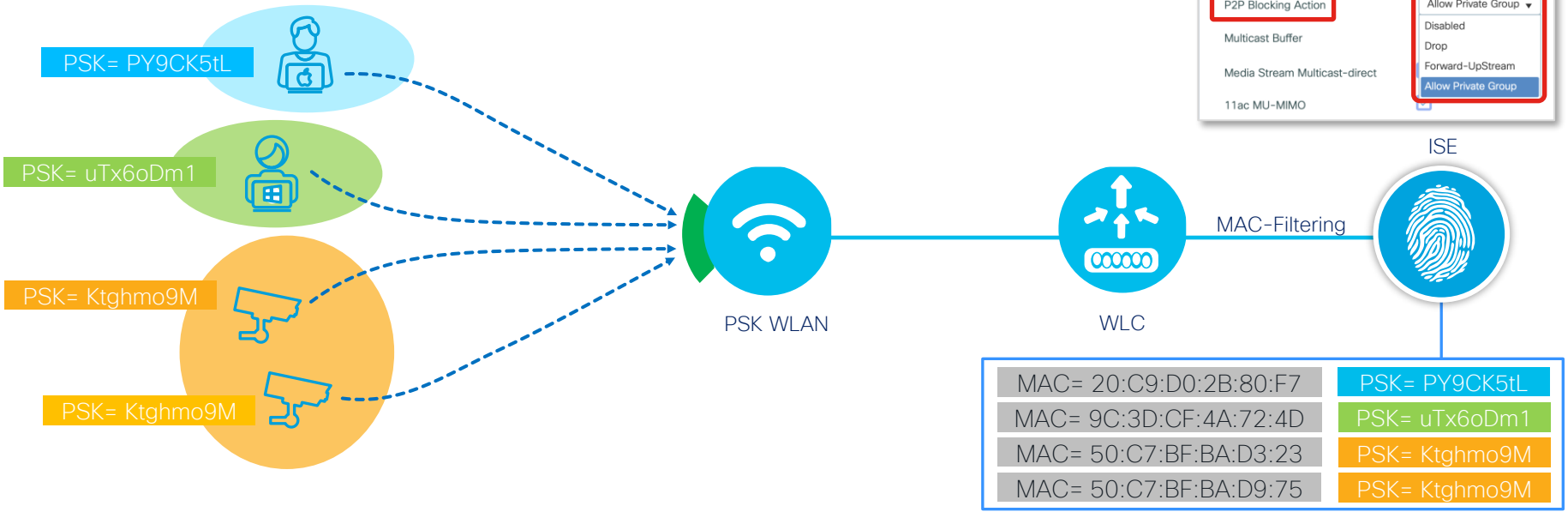
Pre-Shared Key

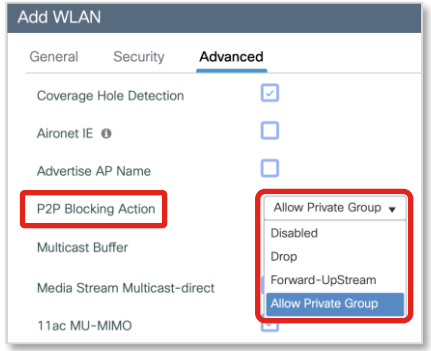


- Offline Attacks
  - Dictionary
  - Rainbow Table
- Strong Passwords Matter

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

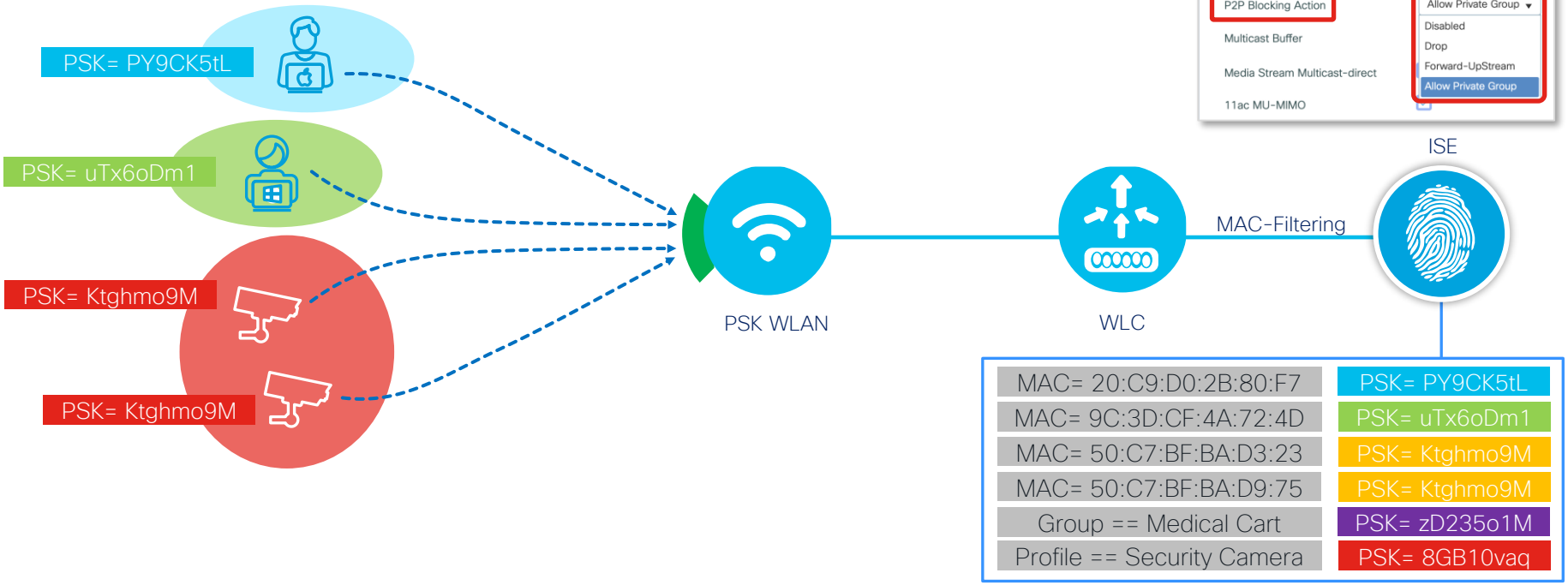
Identity PSK





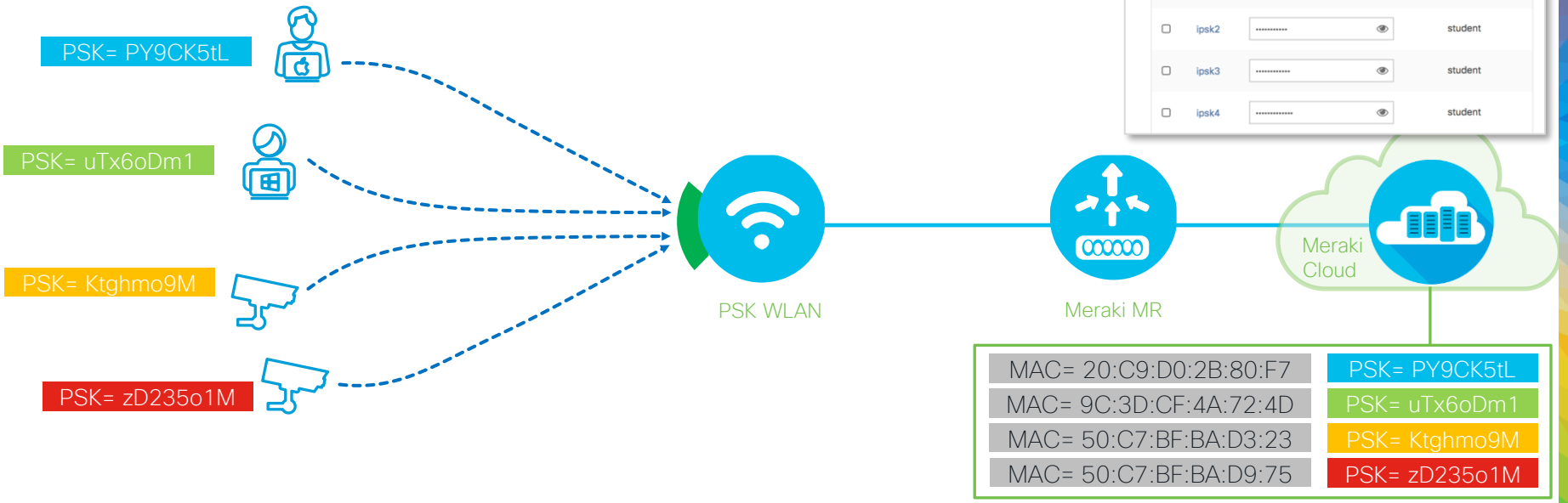
https://www.cisco.com/c/en/us/support/docs/wireless/catalyst-9800-series-wireless-controllers/216130-configure-catalyst-9800-wlc-ipsk-with-ci.html
https://documentation.meraki.com/MR/Encryption_and_Authentication/IPSK_with_RADIUS_Authentication

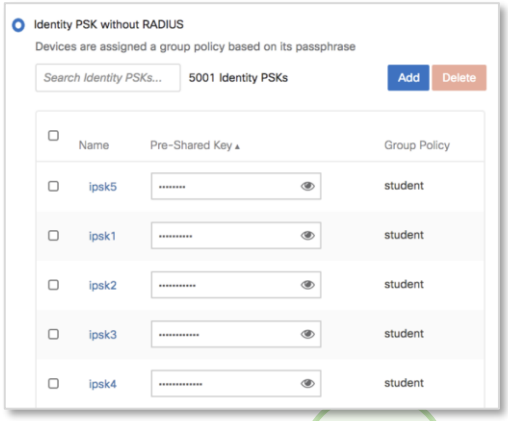
Identity PSK



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

Identity PSK without RADIUS





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

Simultaneous Authentication of Equals

WPA3

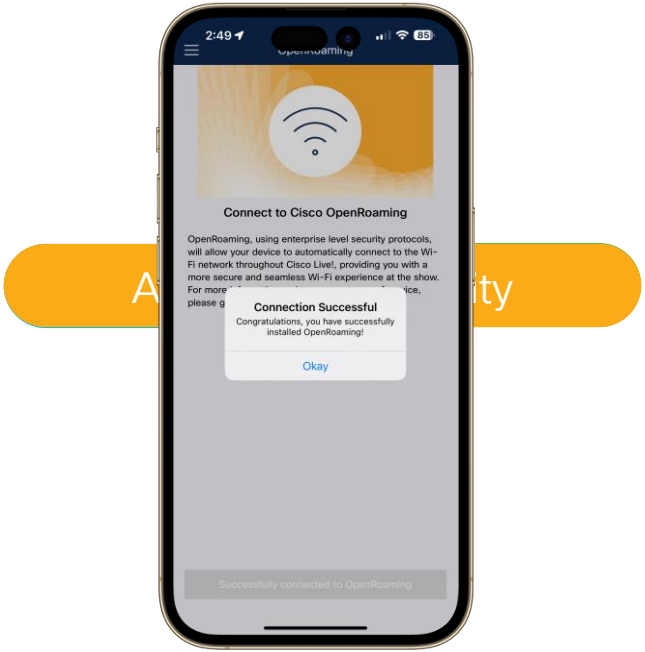
- Based on the Dragonfly Key Exchange
  - Balanced Password Authenticated Key Exchange
    - Security of SAE not tied to the complexity of the shared secret
  - SAE exchanges results in a 32-byte PMK
    - Protects against offline dictionary attacks
    - Forward secrecy protects traffic if the password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

Wi-Fi Certified Enhanced Open

WPA3

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

Decoupling Access and Identity



OpenRoaming

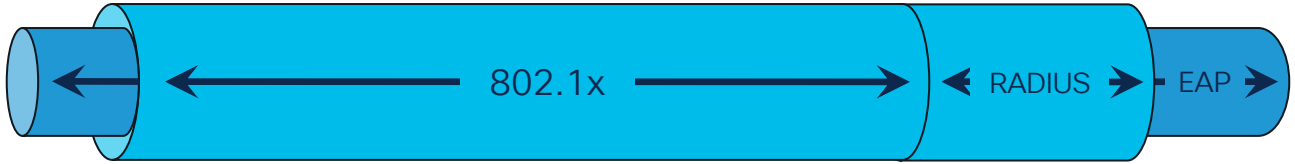
Access

Wireless Network Discovery

OPENROAMING
WIRELESS BROADBAND ALLIANCE

Identity

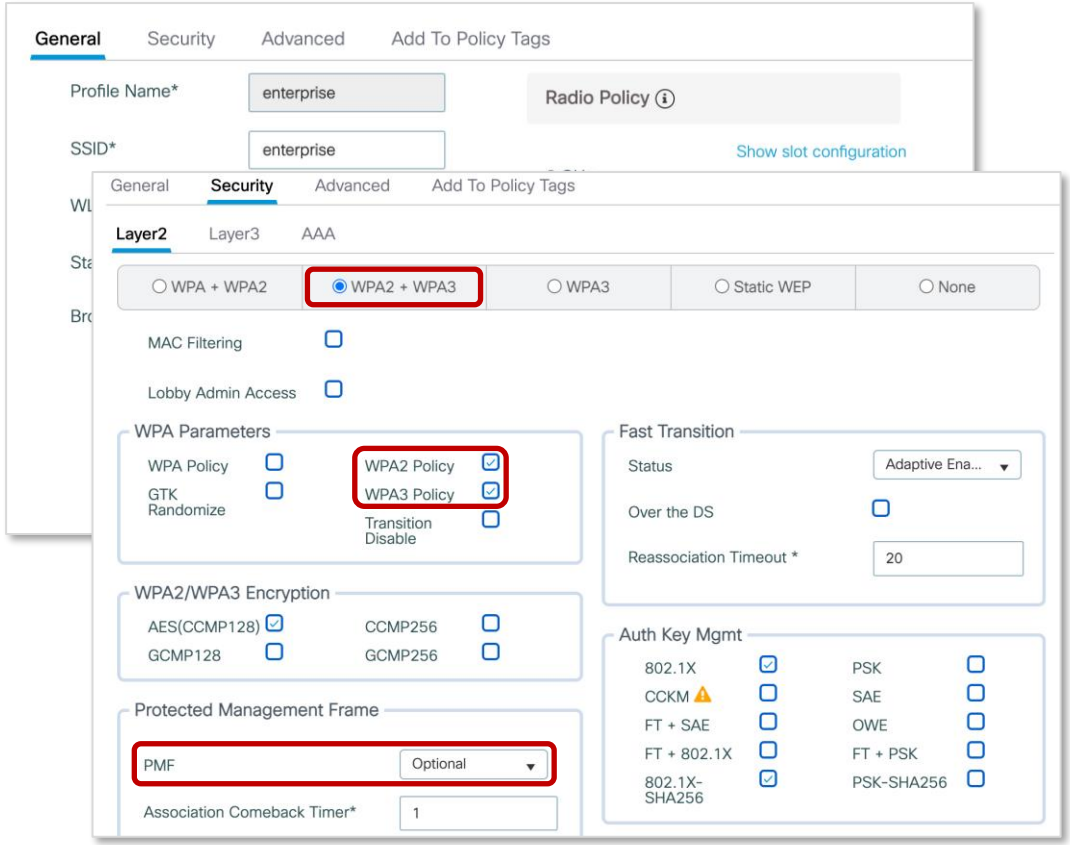
Unique Identity



Implications of 6GHz

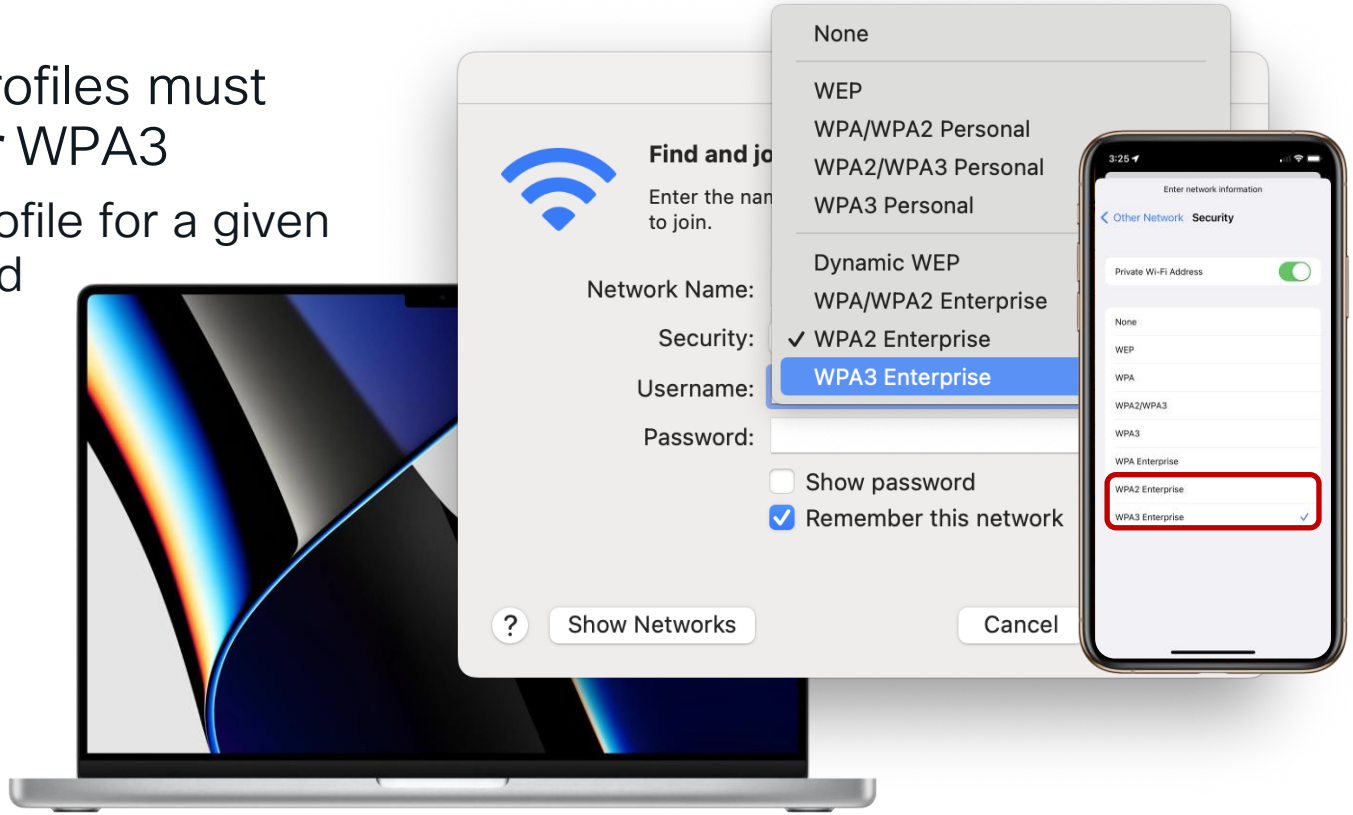
WPA3 and OWE are mandatory for 6GHz

WPA2 and Open are not supported on 6GHz



Wi-Fi 6E and Wi-Fi 7 Security

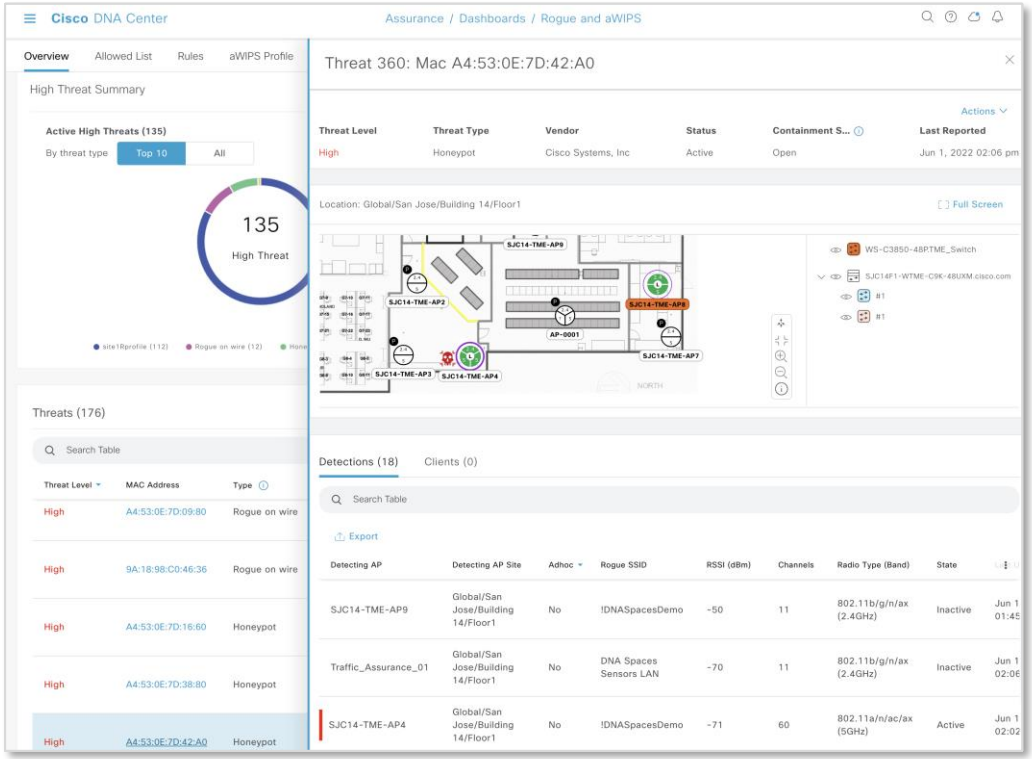
- Client device profiles must select WPA2 ***or*** WPA3
  - And only one profile for a given SSID is permitted



Rogue Detection and Advanced WIPS

Rogue Detection and Advanced WIPS

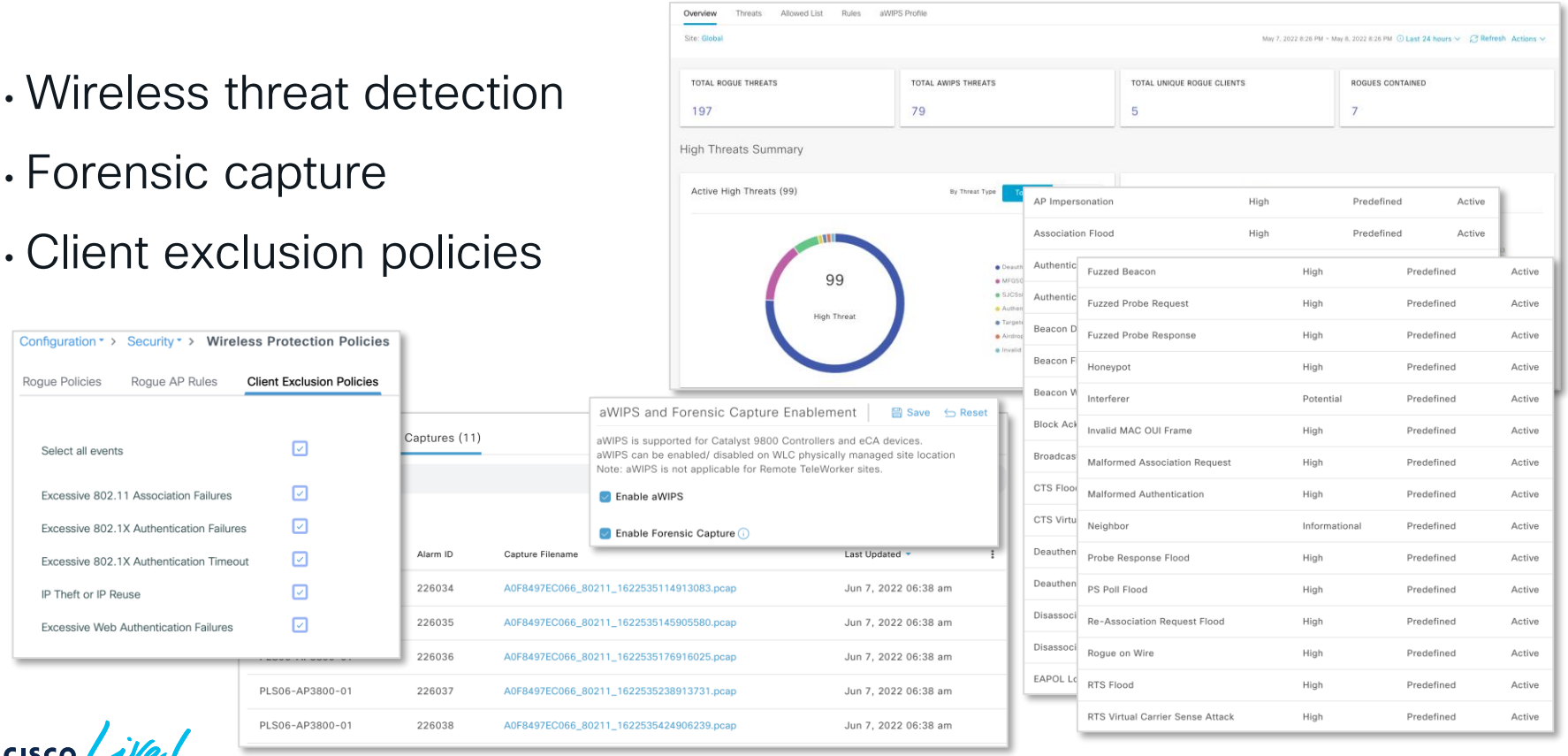
- Centralized wireless threat management
- Rogue detection and classification
- Rogue location and mitigation
- Monitor and classify threats
- Event correlation
- Security compliance reporting



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

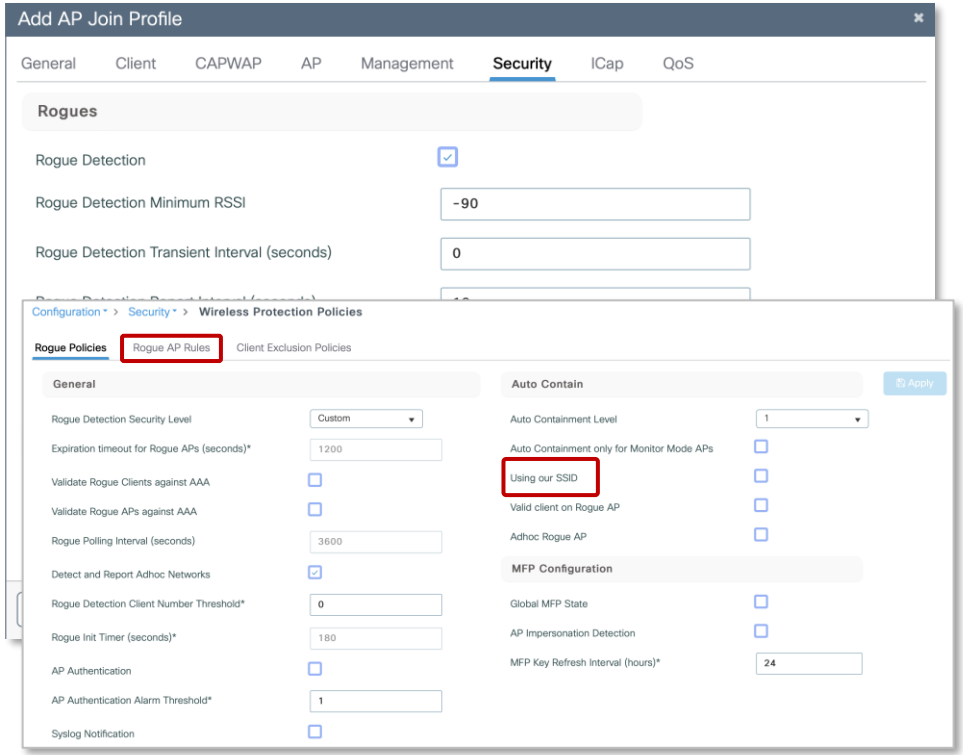
Rogue Detection and Advanced WIPS

- Wireless threat detection
- Forensic capture
- Client exclusion policies



Rogue Access Points

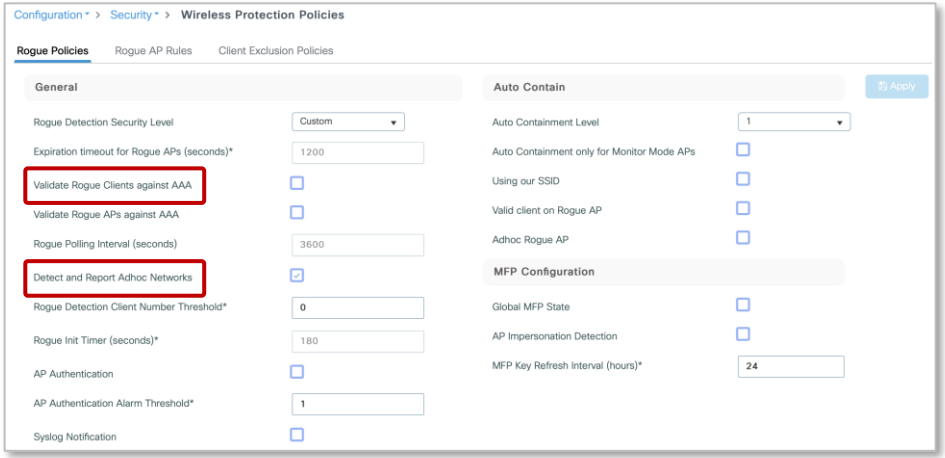
- A Rogue AP is any AP which is not part of our infrastructure
  - Most of them will be legitimate
  - Some of them may be malicious
  - Correctly differentiating between the two is critical



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



Cisco Catalyst Centre Threat Levels

Informational

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

Potential

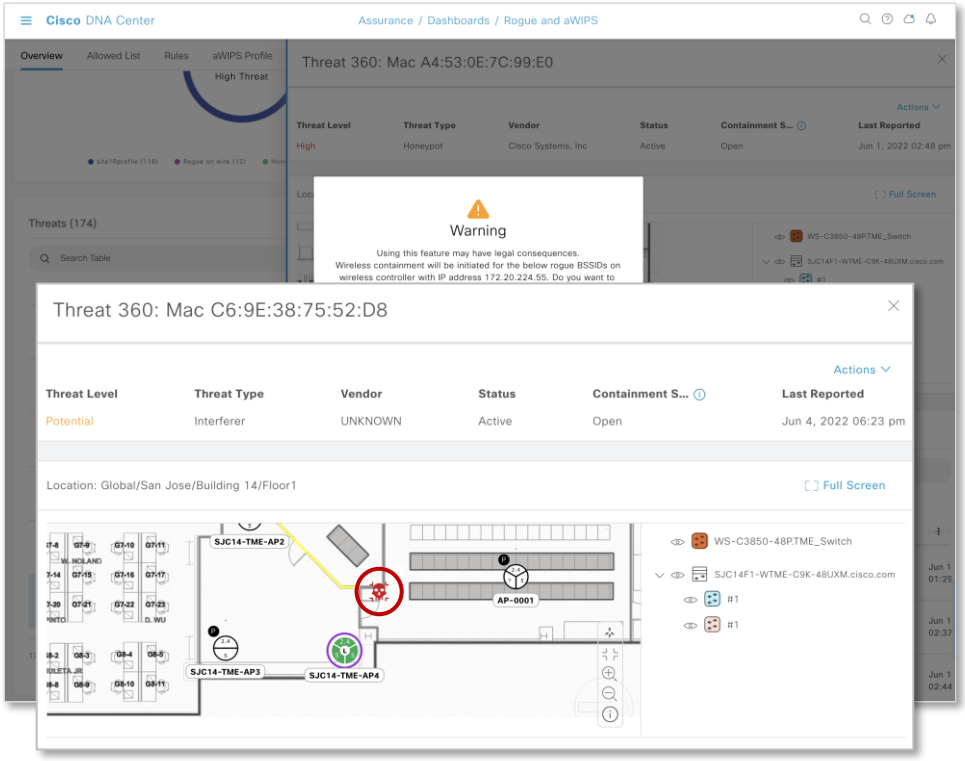
- RSSI >-75 dBm and not on wire
- Rogue Type: Interferer

High

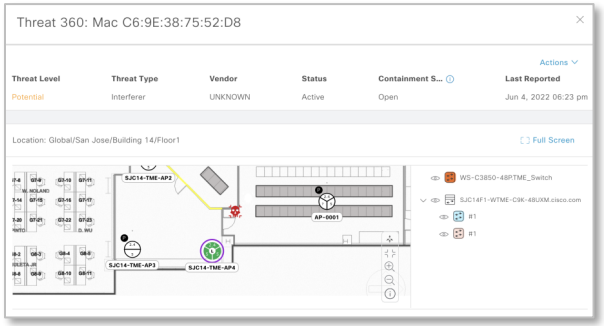
- Rogue Types
  - Honeypot
  - Impersonation AP
  - Rogue on wire
  - Beacon DS attack
- All WIPS threats

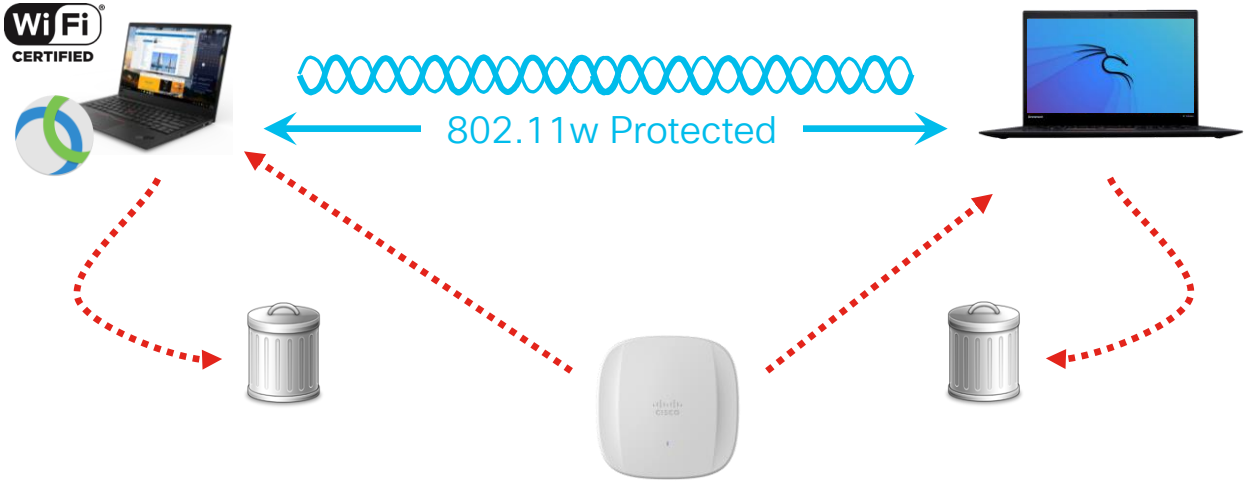
Rogue AP Containment

- 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



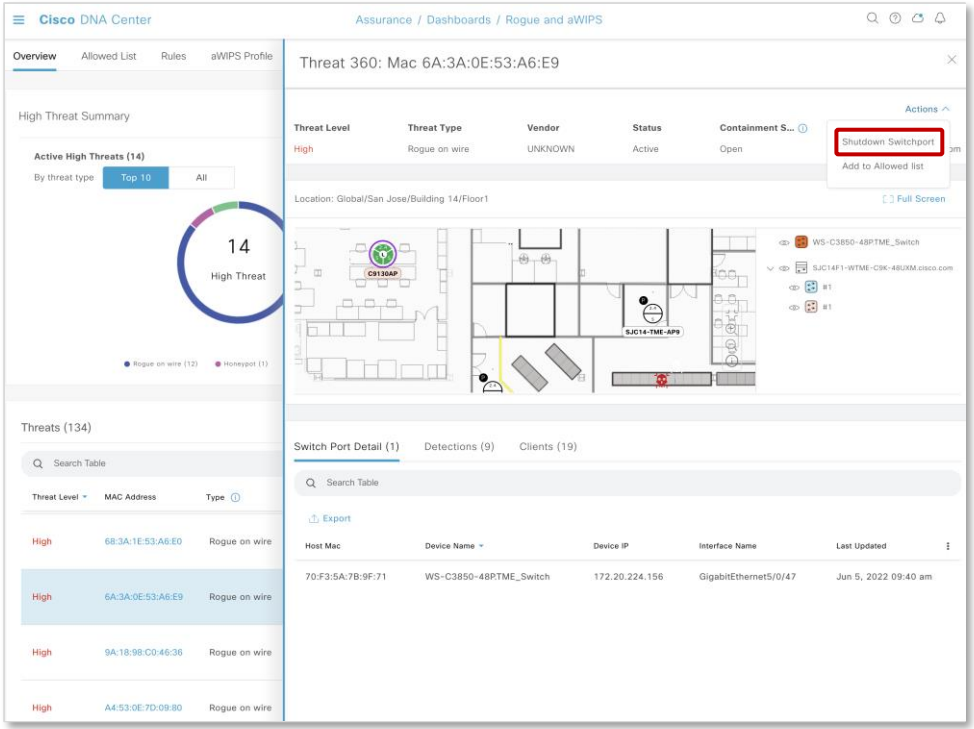
Rogue Containment with WPA3





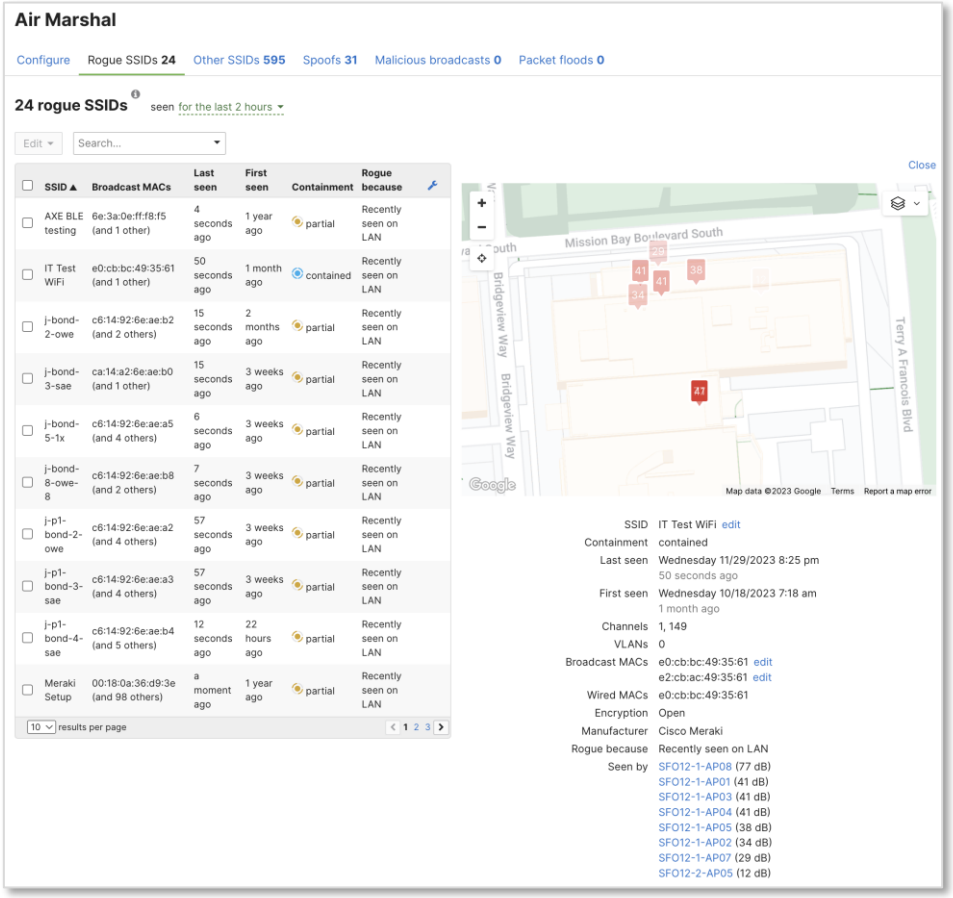
Rogue on Wire

- Matching Algorithms
  - MAC Address ±3/±2/±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



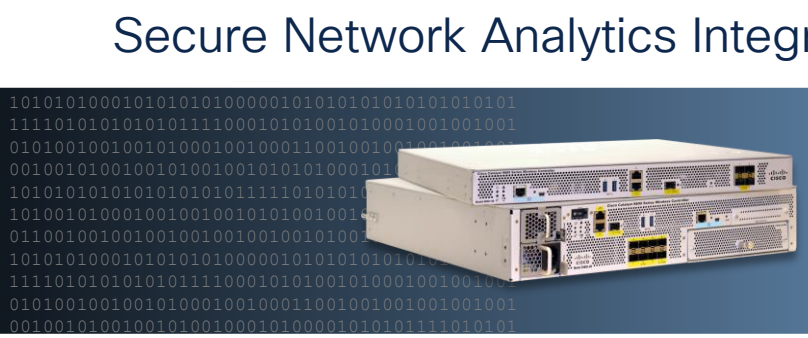
Air Marshal

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



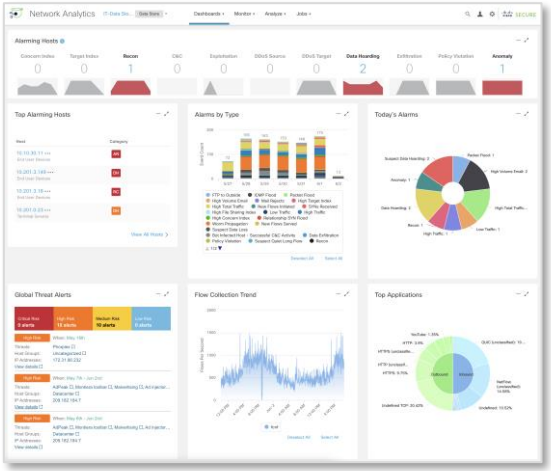
Network as a Sensor

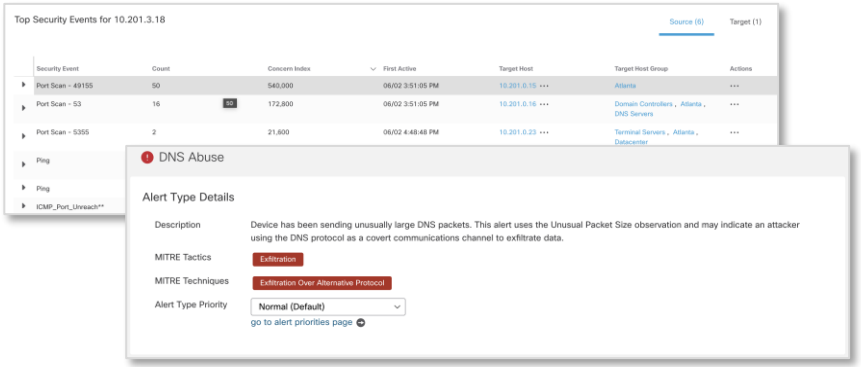
Secure Network Analytics Integration



Netflow

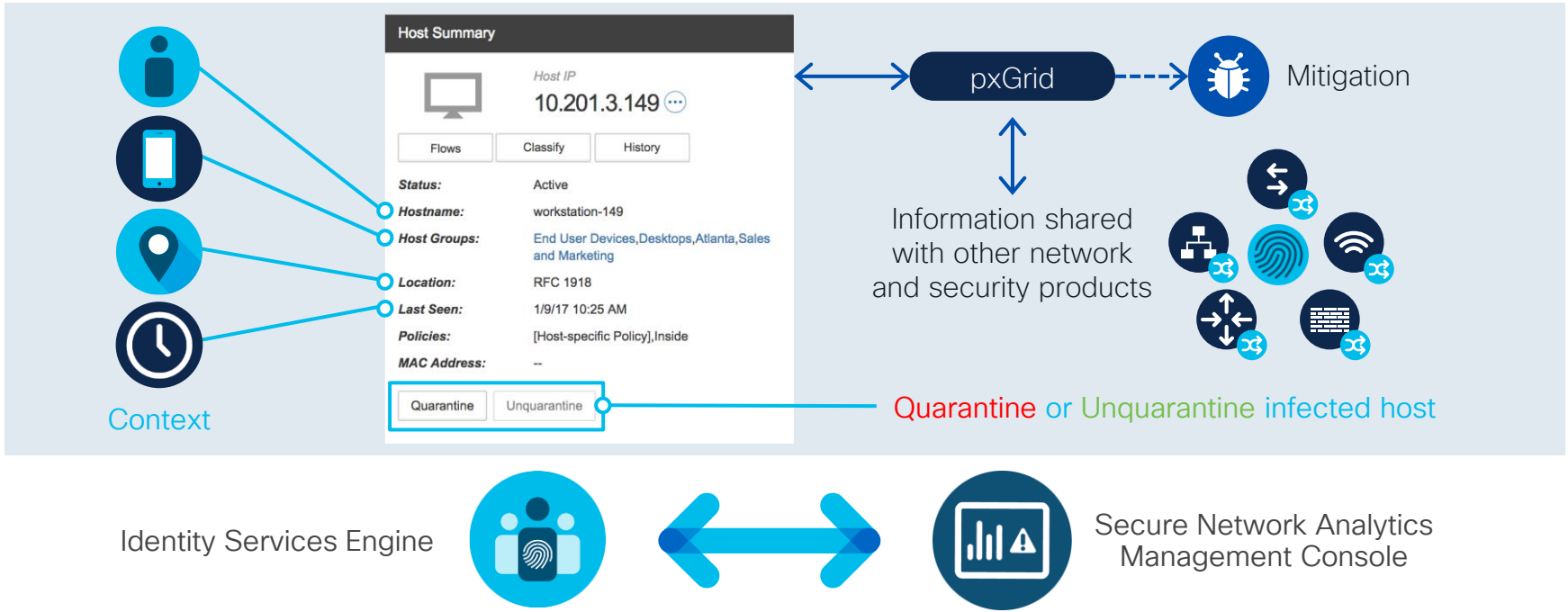
Malware detection and cryptographic compliance on Cisco Stealthwatch





Network as an Enforcer

Rapid Threat Containment

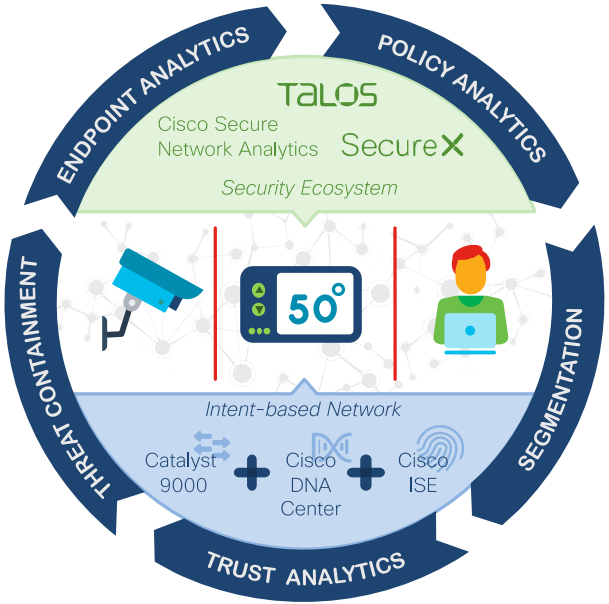


Securing the Wireless Network

Secure the Air

Secure the Devices

Secure the Network




cisco
The bridge to possible
Thank you
cisco Live!

Continue your education

START

Monday, February 5 | 2:15 p.m.
TECEWN-3369
TAC stories : WiFi networks that save lives...and your job

Tuesday, February 6 | 8:00 a.m.
BRKEWN-2014
Meraki Wireless AIOps - An Intuitive AI Solution to Optimize Wi-Fi at Scale !

Tuesday, February 6 | 4:45 p.m.
BRKEWN-2029
Cisco Wireless AIOps

Wednesday, February 7 | 4:00 p.m.
BRKEWN-2097
Monitoring Catalyst Wireless with the Meraki Dashboard

Thursday, February 8 | 10:45 a.m.
BRKEWN-2667
Cisco Wireless Supercharged by Cisco Catalyst Center - The Ultimate Guide to Bring Your Wireless Operation to the Next Level

Thursday, February 8 | 1:30 p.m.
BRKEWN-2043
Saving Energy and Money with Your Cisco Wireless Network

Friday, February 9 | 9:00 a.m.
BRKEWN-3628
Troubleshoot Catalyst 9800 Wireless Controllers

Friday, February 9 | 11:00 a.m.
BRKEWN-2399
Meraki Wireless from a Troubleshooter Perspective

FINISH

Friday, February 9 | 11:00 a.m.
BRKEWN-3006
Keep your Catalyst 9800 & AP-COS Wireless Network Healthy, with Wireless Config Analyzer Express and other Advanced Tools

Continue your education

START

Monday, February 5 | 8:30 a.m.
TECEWN-2005
Secure, Scalable, Enterprise Wi-Fi Deployment using Meraki Cloud

Tuesday, February 6 | 11:45 a.m.
IBOEWN-2031
The Inner Workings of QoS for Modern Wireless Networks

Tuesday, February 6 | 1:15 p.m.
BRKEWN-2926
Tune your Cisco Wi-Fi designs for the most demanding clients and applications, boosted with applied AI

Tuesday, February 6 | 2:00 p.m.
IBOEWN-2000
Design/Deployment and tuning of Outdoor Wi-Fi & Workgroup Bridges (WGBs)

Tuesday, February 6 | 4:45 p.m.
BRKEWN-2035
Meraki Wireless: Ready for Enterprise

Wednesday, February 7 | 2:15 p.m.
BRKEWN-2042
Cisco Spaces: How to Turn your Wi-Fi Network into Location Based Intelligence

Wednesday, February 7 | 2:15 p.m.
IBOEWN-2349
An Open Discussion on Shaping the Future of Buildings with Cisco Spaces

Thursday, February 8 | 8:30 a.m.
BRKEWN-3004
Understanding Wireless Security and the Implications for Secure Wireless Network Design

Thursday, February 8 | 8:45 a.m.
BRKOPS-2402
Automate the Deployment of a Wireless Network with the Help of Cisco Catalyst Center

FINISH

Thursday, February 8 | 5:00 p.m.
BRKEWN-2037
Open Roaming under the hood


cisco Live!
Let's go