

CISCO *Live!*

ALL IN

#CiscoLiveAPJC



The bridge to possible

Understanding Wireless Security

And the Implications for Secure Wireless Network Design

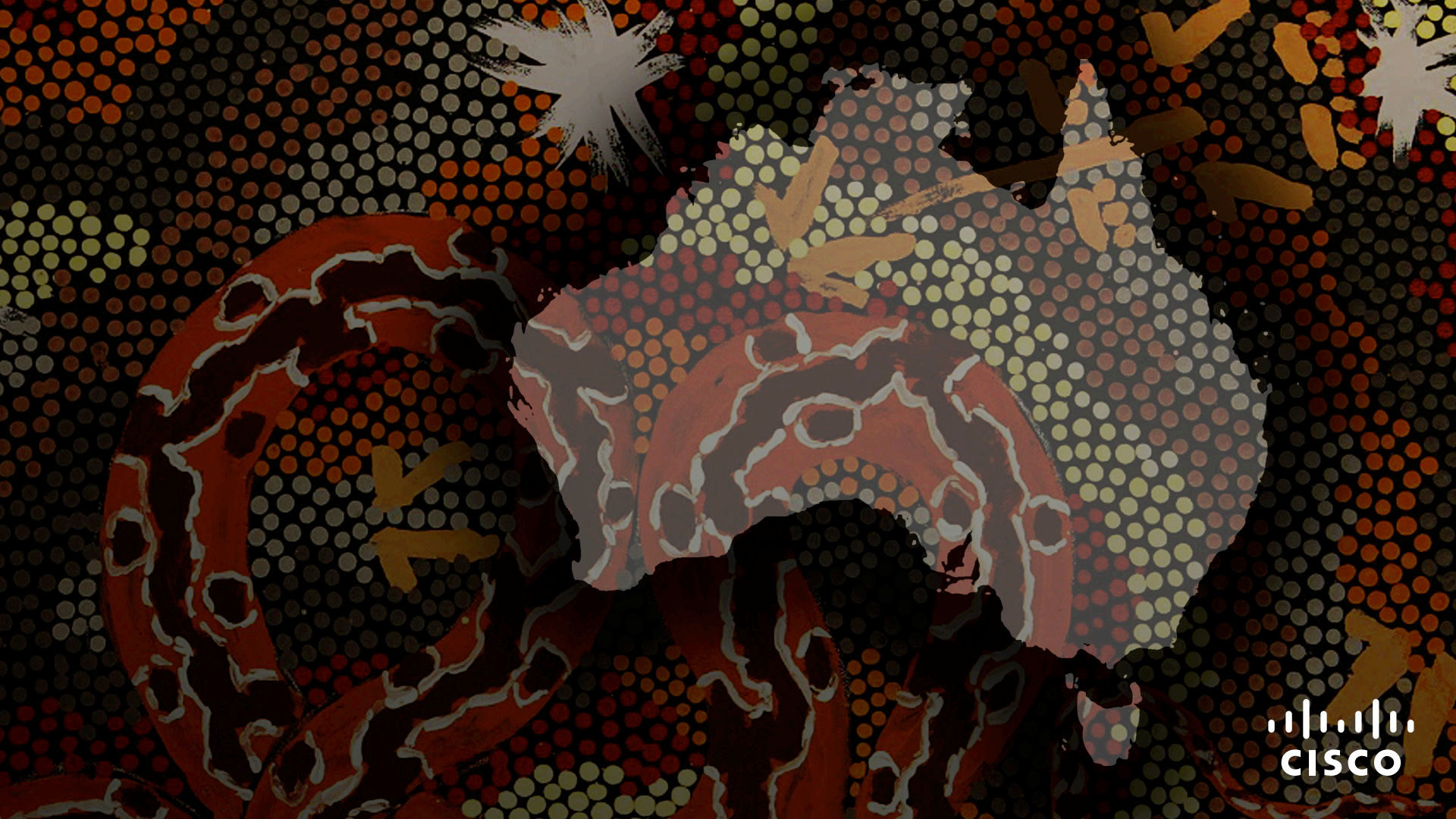
Mark Krischer

Principal Wireless Architect, Asia Pacific, Japan & Greater China

BRKEWN-3004

CISCO *Live!*

#CiscoLiveAPJC



Cisco Webex App

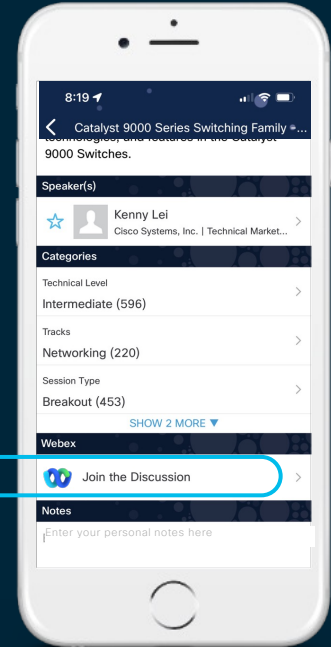
Questions?

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 Thursday 22 December, 2022.



<https://cicolive.ciscoevents.com/cicolivebot/#BRKXXX-xxxx>



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.

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.

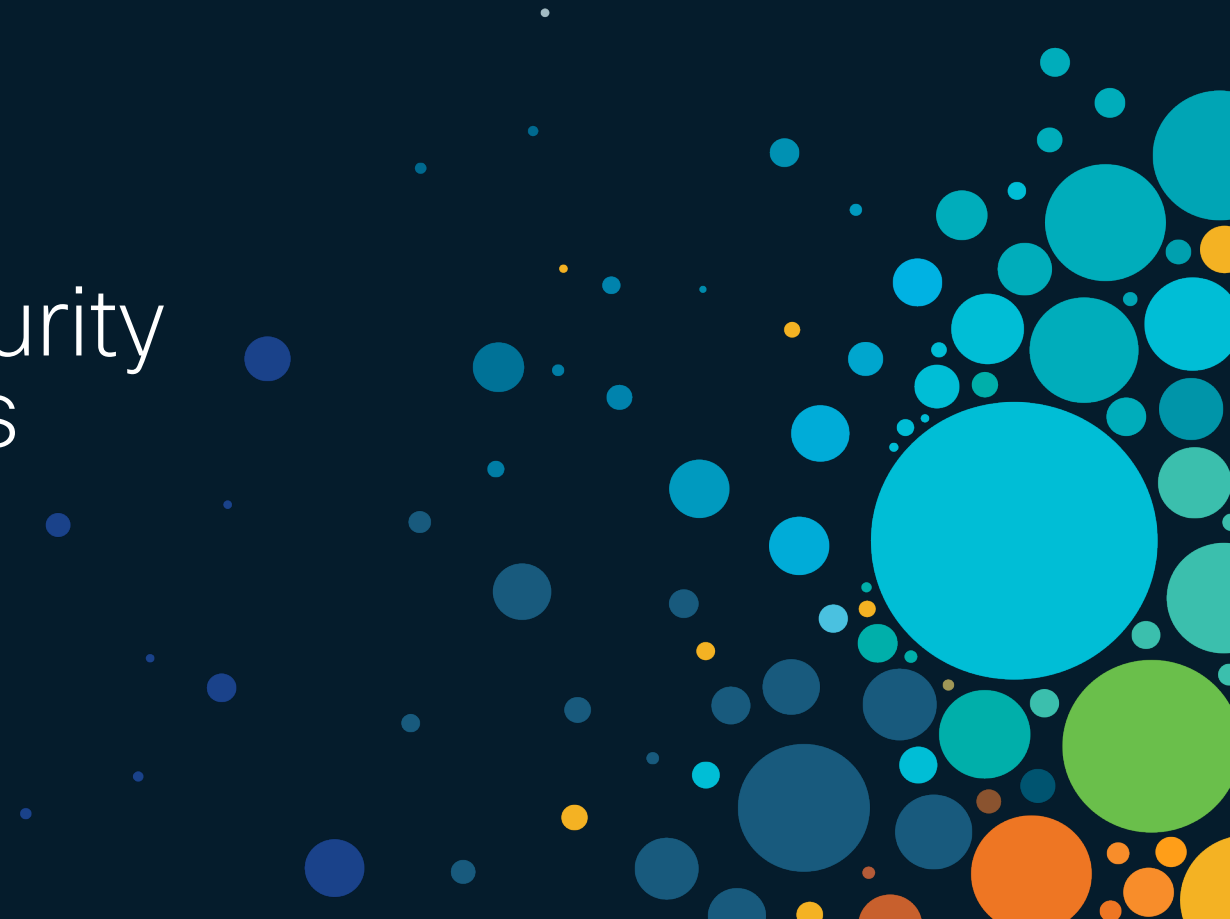
The intent is to provide a deeper understanding, not just about the security capabilities themselves, but to do so from the perspective of the attacks that they defend against.



Agenda

- Wireless Security Fundamentals
 - WPA3
 - Authentication and Authorisation
 - 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

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)

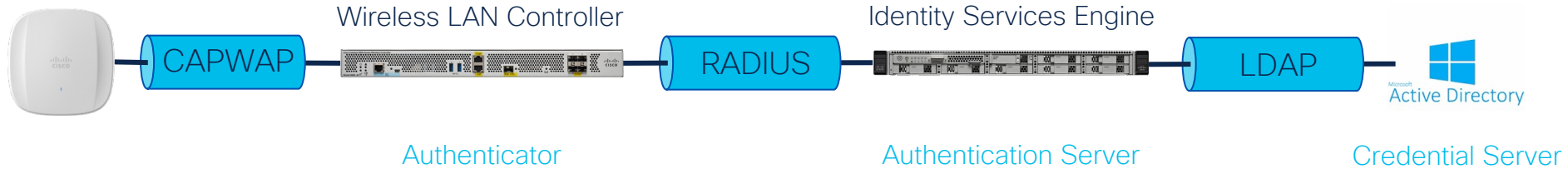
802.11 Fundamentals

Authentication



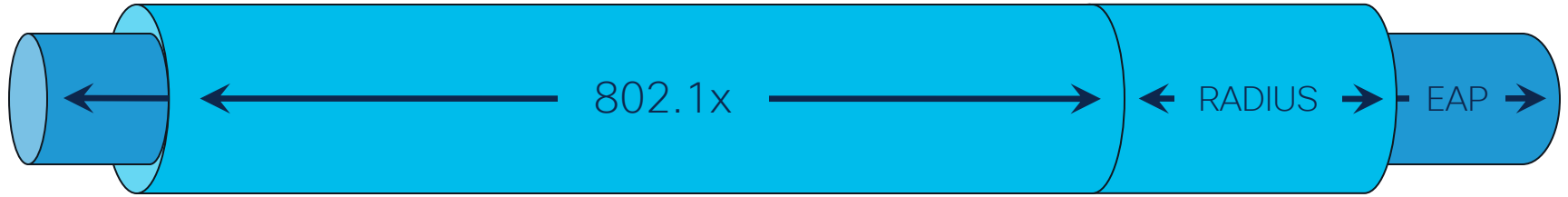
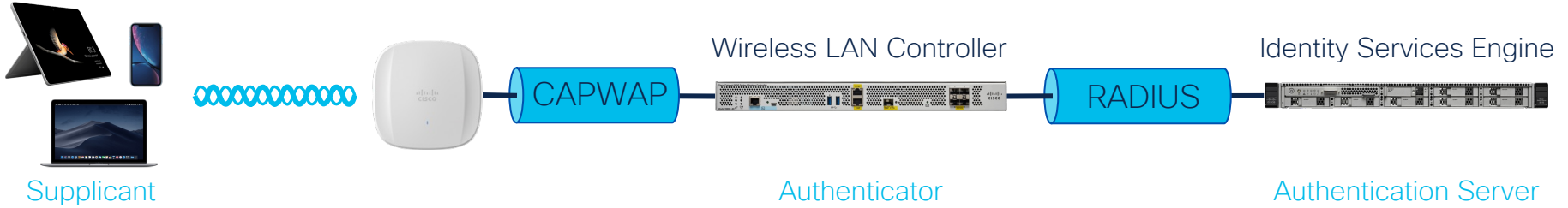
802.11 Fundamentals

Authentication



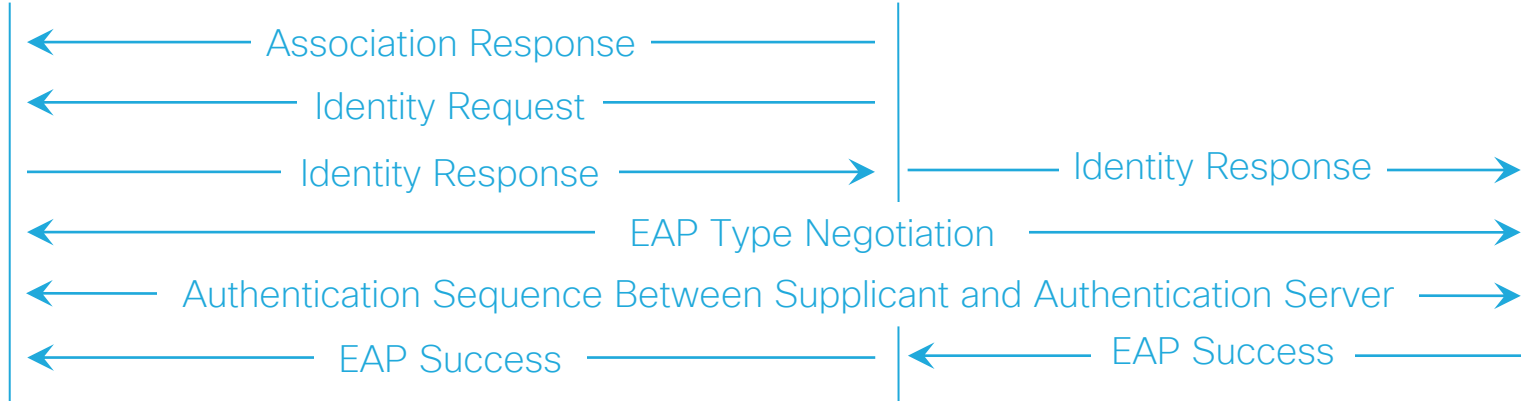
802.11 Fundamentals

Authentication



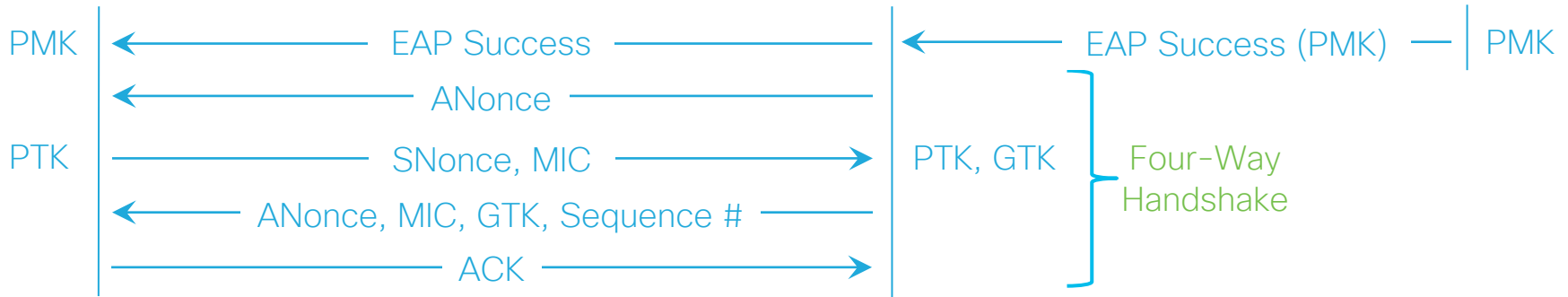
802.11 Fundamentals

Authentication



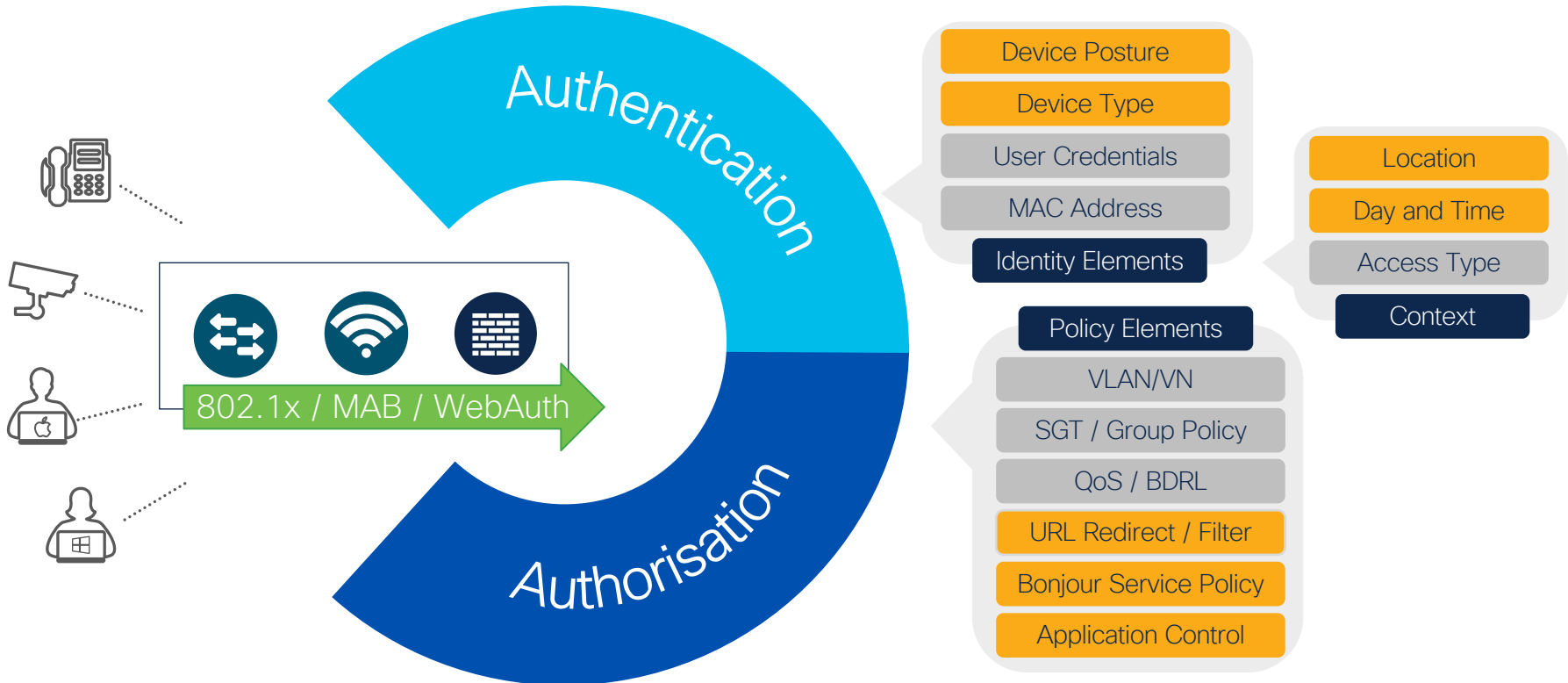
802.11 Fundamentals

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

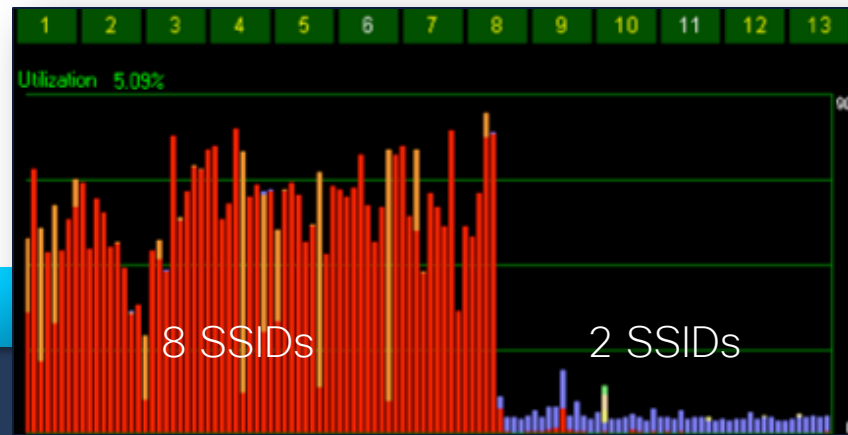
Assigns multiple access characteristics: VLAN, ACL, QoS, Timer, etc.

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)

On-Prem and Cloud Identity Providers



On-Prem Identity Provider



802.1x, Network Access



MSCHAPv2, PAP
EAP-FAST, EAP-TLS
MAC Filtering



Cloud Identity Provider



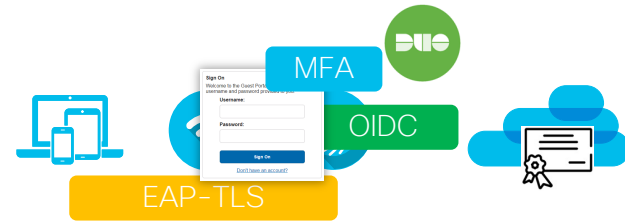
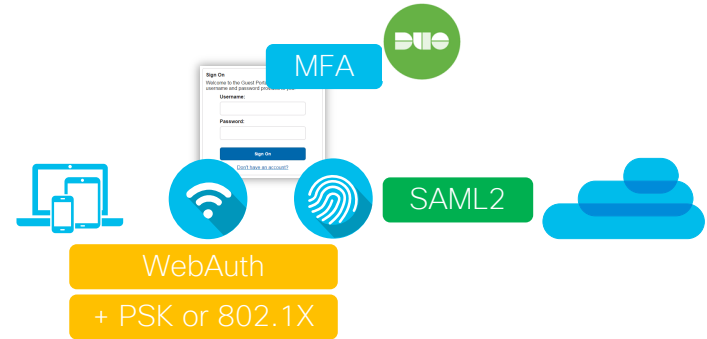
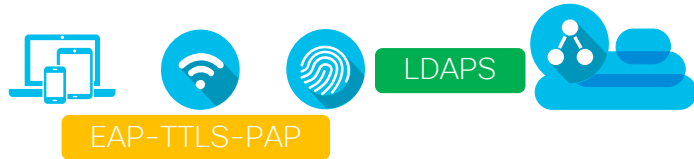
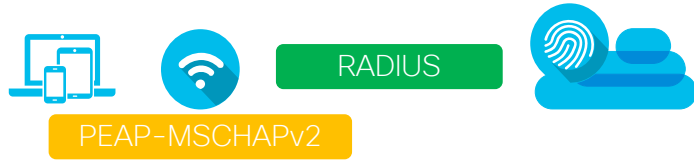
VPN, Applications



SAMLv2, OpenID Connect



Cloud Identity and Multi-Factor Authentication



Multi-Factor Authentication



What type of device are you adding?

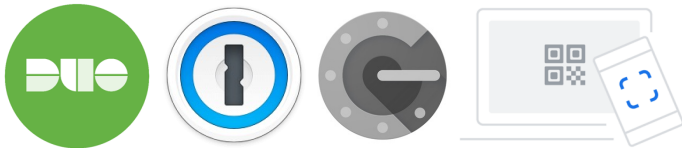
- Mobile phone** RECOMMENDED
- Tablet** (iPad, Nexus 7, etc.)
- Security Key** (YubiKey, Feitian, etc.)
- Touch ID**
Requires Chrome to use Touch ID.

[What is this?](#) [Need help?](#)

Powered by Duo Security

Continue

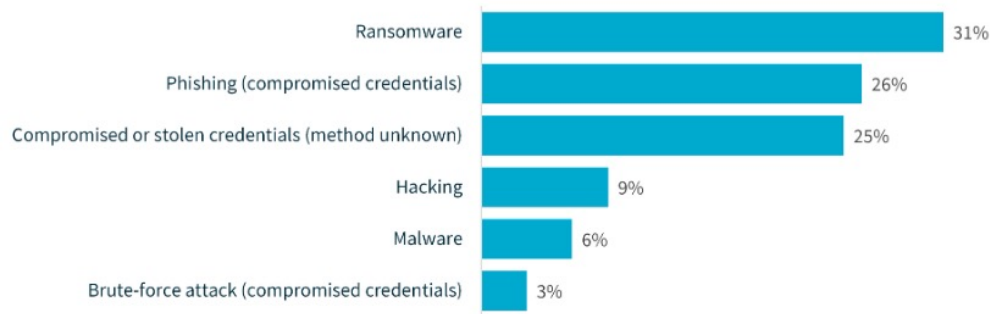
- Push notification for ease simplified access
- Requires network access
- Traditional time based one-time passwords
- Manual process



Zero Trust and Wireless Networking

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

Cyber incident breakdown



- Ransomware
 - East/West Traversal
 - Authorisation
 - Micro-segmentation

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

Secure Fast Roaming Challenges



- Client channel scanning and AP selection

- Re-authentication of client device and re-keying

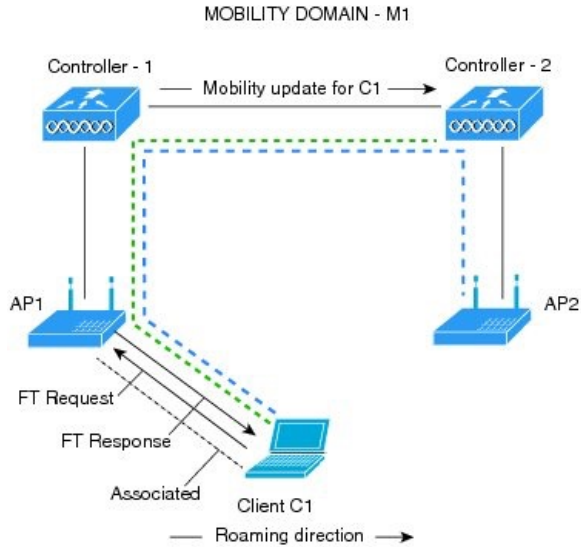
Secure Fast Roaming

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



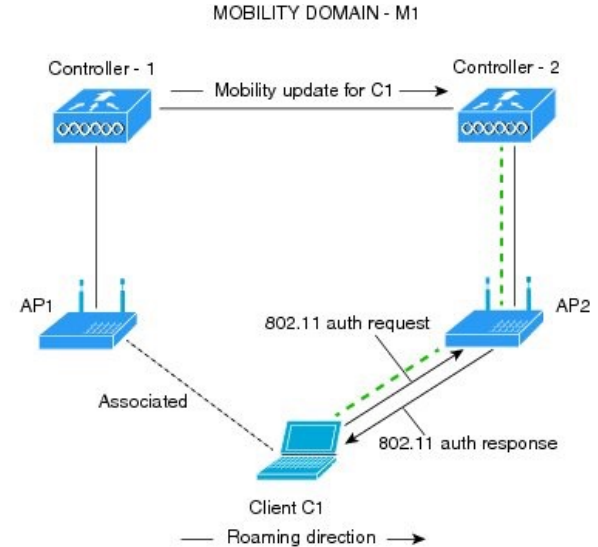
- Client channel scanning and AP selection
 - 802.11k Neighbor Lists based on CCX (Cisco Compatible Extensions)
 - 802.11v BSS Transition
- Re-authentication of client device and re-keying
 - 802.11r Fast BSS Transition based on CCKM (Cisco Centralised Key Management)

802.11r Fast Transition



- - - - Client's logical FT communication
- Actual communication path

Over the DS



- Actual communication path

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, indicating the configuration for 802.11r. The 'Status' dropdown is set to 'Enabled', and the 'Over the DS' checkbox is unchecked. Other security options like WPA2 + WPA3, WPA Parameters, WPA2/WPA3 Encryption, and Protected Management Frame are also visible.

Section	Option	Value/Status
Fast Transition	Status	Enabled
	Over the DS	Off
	Reassociation Timeout	20
	WPA Parameters	WPA2 Policy: On, WPA3 Policy: On, WPA Randomize: Off, Transition Disable: Off
	WPA2/WPA3 Encryption	AES(CCMP128): On, GCMP128: Off, CCMP256: Off, GCMP256: Off
Auth Key Mgmt	802.1x	Off
	CCKM	Off
	OWE	Off
	802.1x-SHA256	Off
Protected Management Frame	PMF	Required
	PSK	Off
Auth Key Mgmt	SAE	Off
	FT + 802.1x	On



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](#)

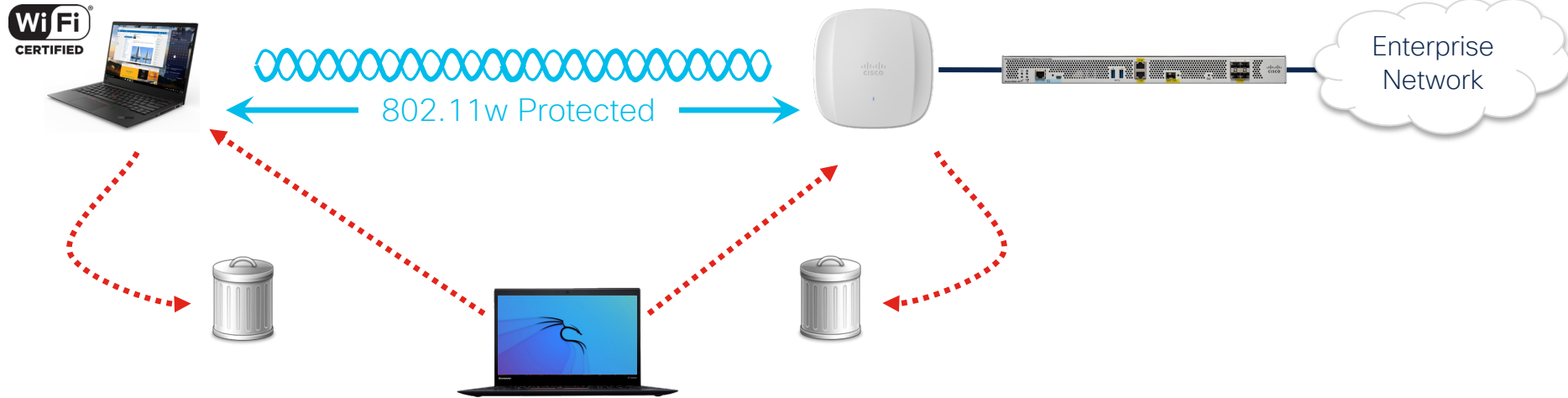
- This was an industry wide issue
 - Not specific to any one vendor
- WPA3 certification includes KRACK exploit testing
- The attacker positions a rogue AP clone to perform a MitM attack
 - This flaw causes all WPA2 encryption protocols to reuse the keystream when encrypting packets
- Rogue AP detection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

KrØØk Vulnerability



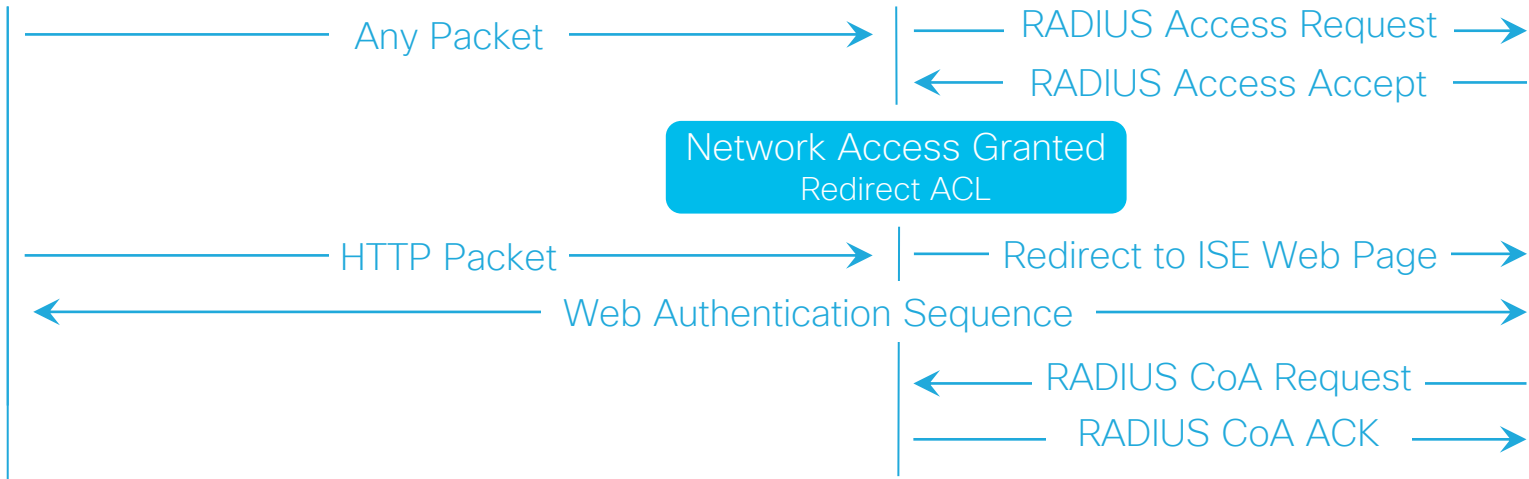
- On February 26th, 2020, researchers Štefan Svorencík and Robert Lipovsky [disclosed a vulnerability in the packet processing of certain Wi-Fi chipsets](#)
- This vulnerability could allow an unauthenticated, adjacent attacker to decrypt Wi-Fi frames without the knowledge of the PTK
- After an affected 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



Central Web Authentication

URL Redirect



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

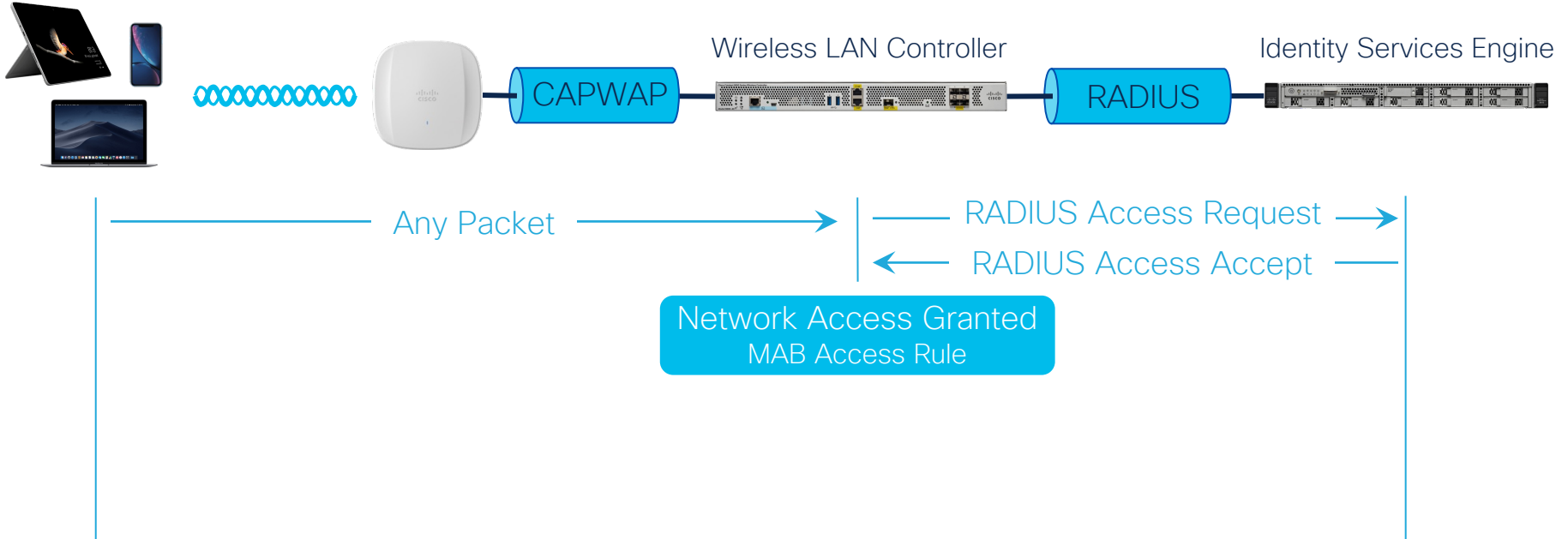


Apple Devices

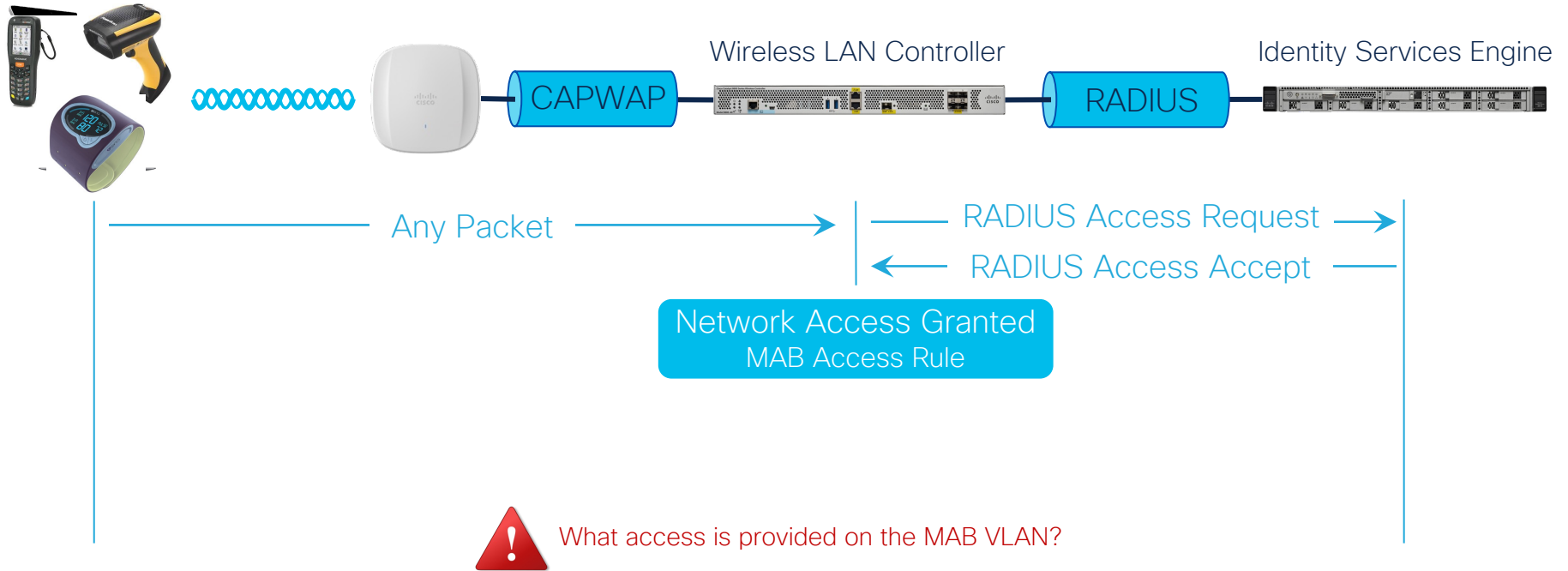
- <http://captive.apple.com/hotspot-detect.html>

Central Web Authentication

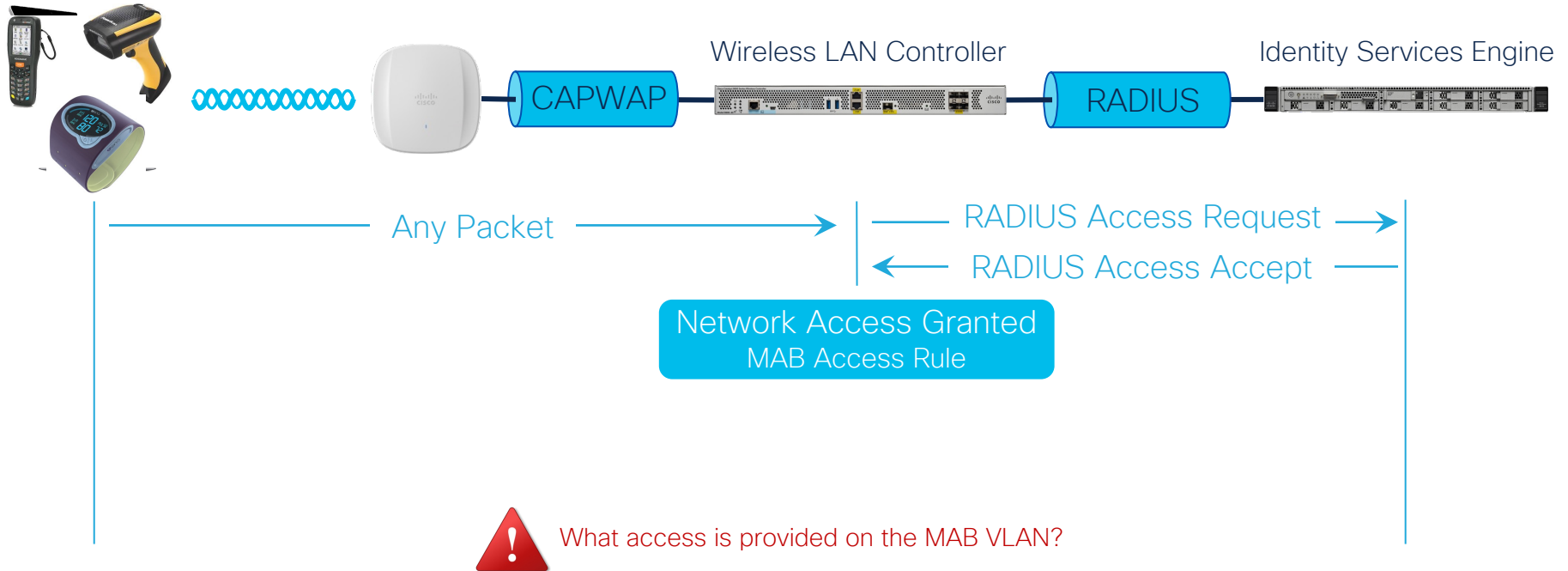
MAC Authentication Bypass



MAC Authentication Bypass



MAC Authentication Bypass



Wi-Fi Certified Easy Connect

WPA3



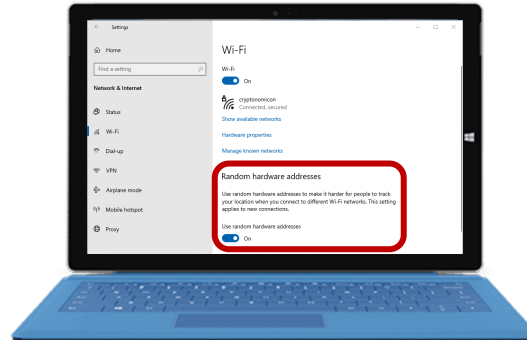
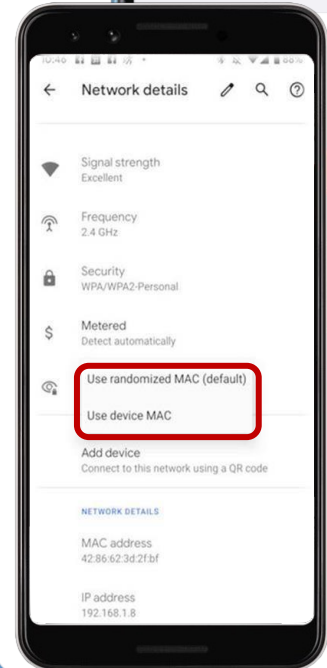
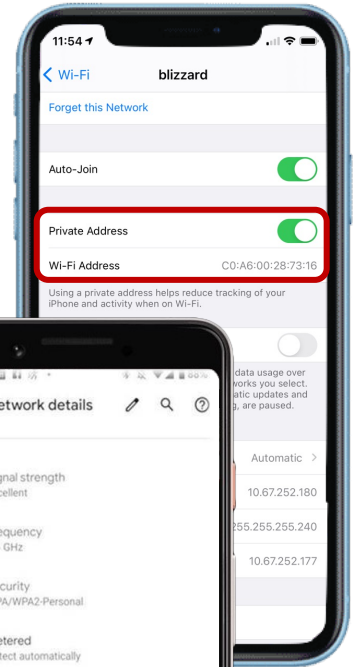
Device Provisioning Protocol (DPP)

- 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



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








Different OS Implementations



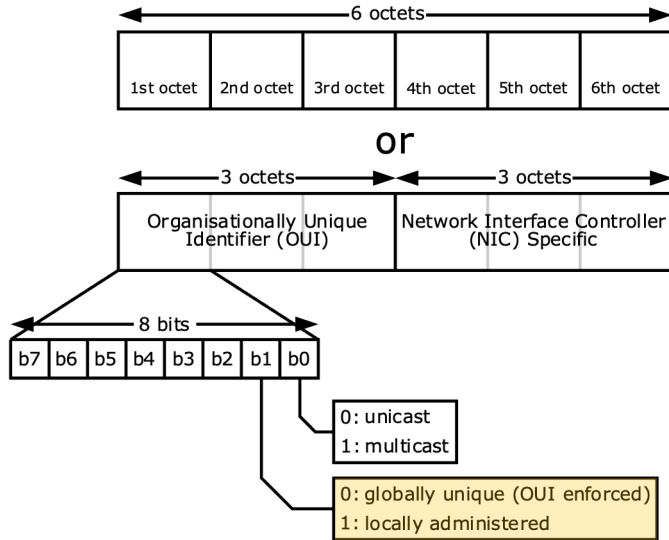
	Windows 10+	Android 10+	iOS 14+, iPadOS 14+, watchOS 7+
Randomization enabled by default	No	Yes	Yes
Same random MAC used for subsequent connection	Yes	Yes	Yes
Randomization saved between device reboot	Yes	Yes	Yes
Random MAC saved when Wi-Fi profile recreated	No	Yes	Yes
Randomization per day and/or per 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>

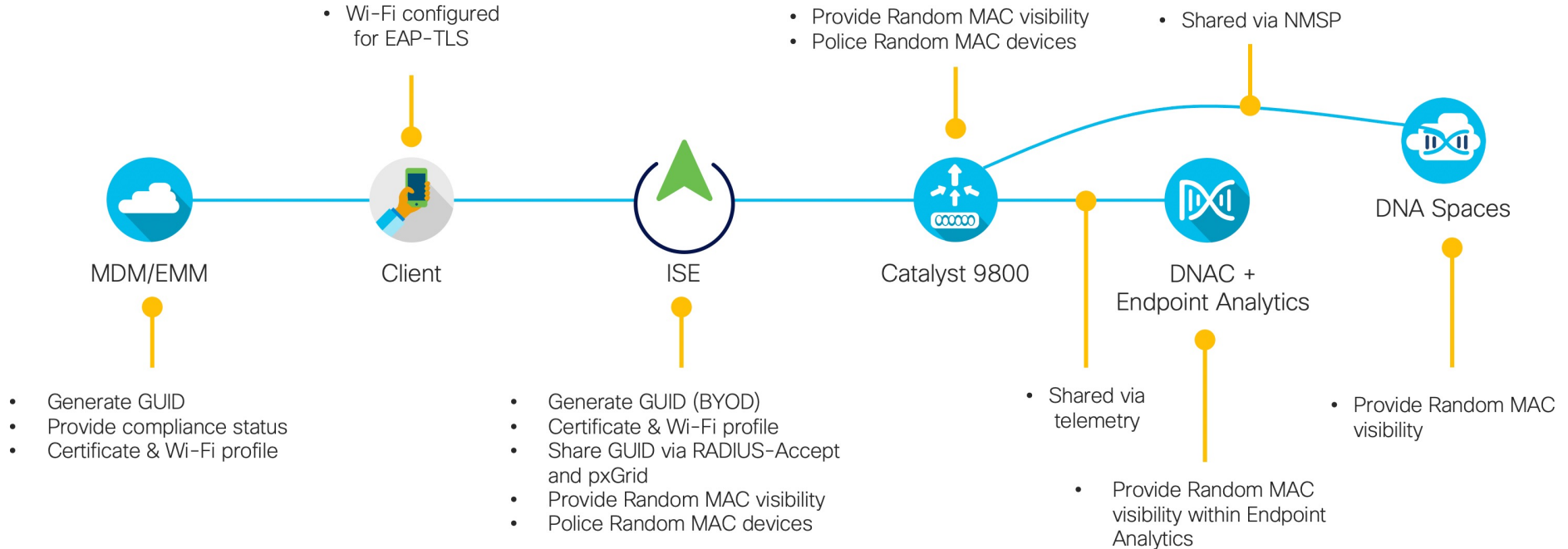
Detecting Random MAC Addresses



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>

Addressing Random MAC Issues

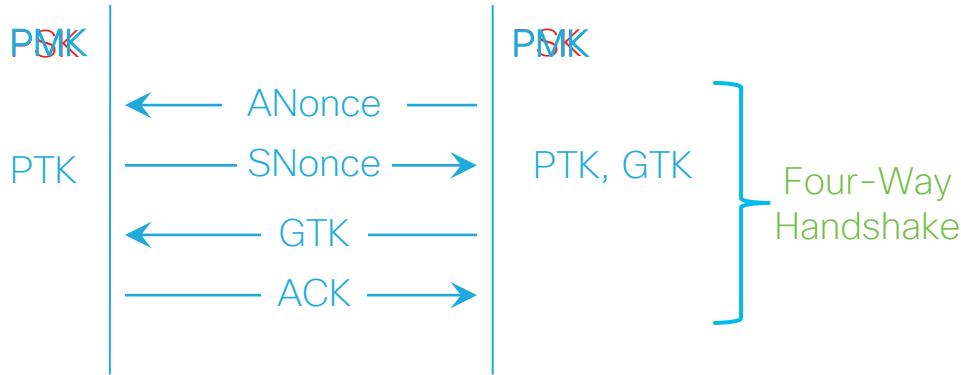


WPA Personal

Pre-Shared Key

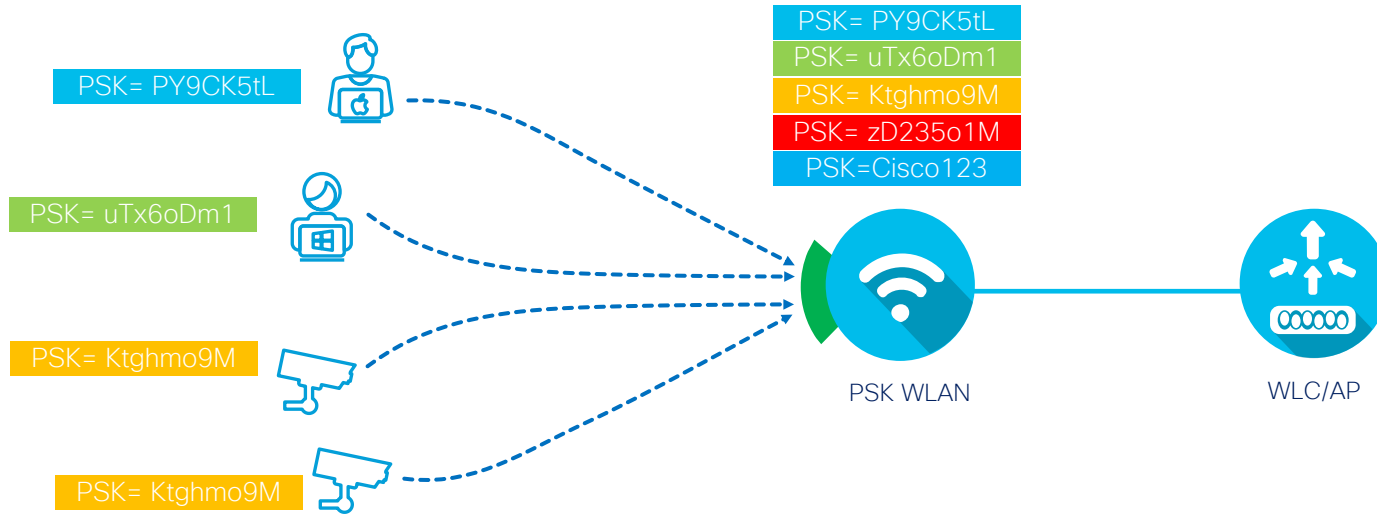


- Offline Attacks
 - Dictionary
 - Rainbow Table
- Strong Passwords Matter

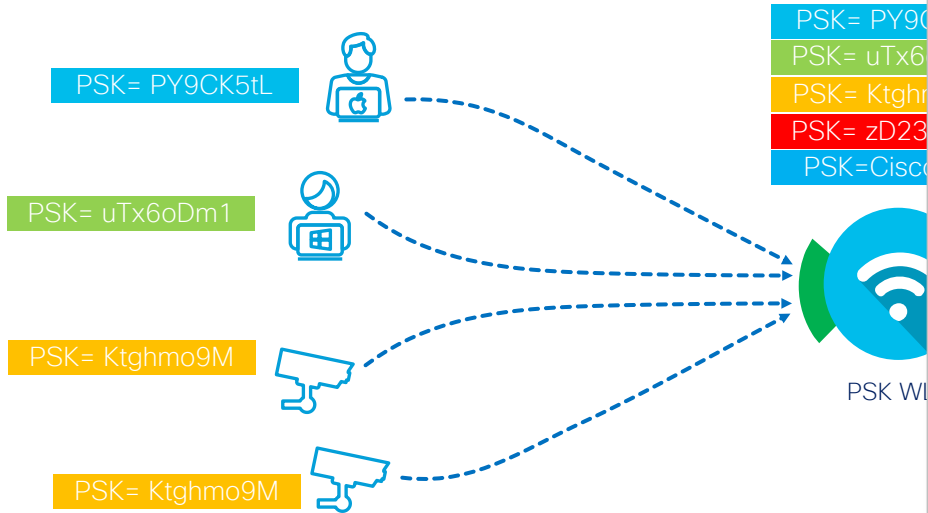


$$PTK = \text{SHA}(\text{PMK} + \text{ANonce} + \text{SNonce} + \text{AP MAC} + \text{STA MAC})$$

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 None

MAC Filtering Authorization List* mpsk

Lobby Admin Access

WPA Parameters

WPA Policy WPA2 Policy

GTK Randomize OSEN Policy

WPA2 Encryption

AES(CCMP128) CCMP256

GCMP128 GCMP256

Protected Management Frame

PMF Disabled

Fast Transition

Status Disabled

Over the DS

Reassociation Timeout * 20

Auth Key Mgmt

802.1x PSK

Easy-PSK CCKM

FT + 802.1x FT + PSK

802.1x-SHA256 PSK-SHA256

PSK Format ASCII

PSK Type Unencrypted

Pre-Shared Key*

MPSK Configuration

Enable MPSK

+ Add - Delete

Priority ▼ Key Format ▼ Password Type ▼

Priority * Priority(0-4)

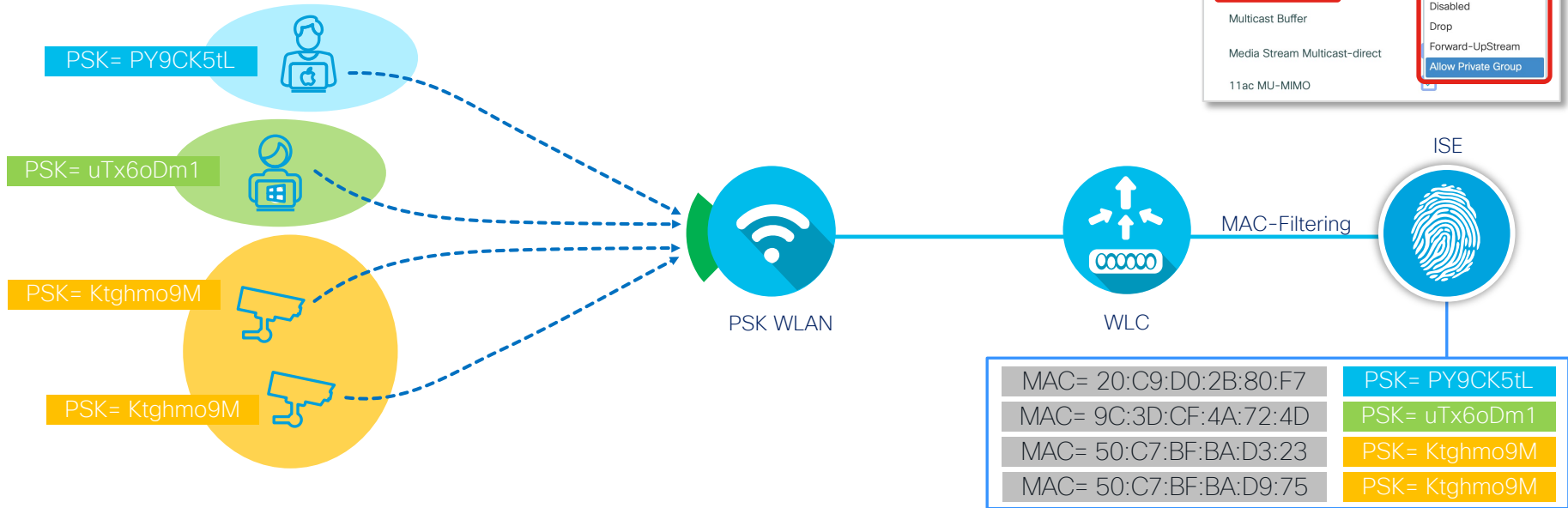
Key Format ASCII

Password Type Unencrypted

Pre-Shared Key*

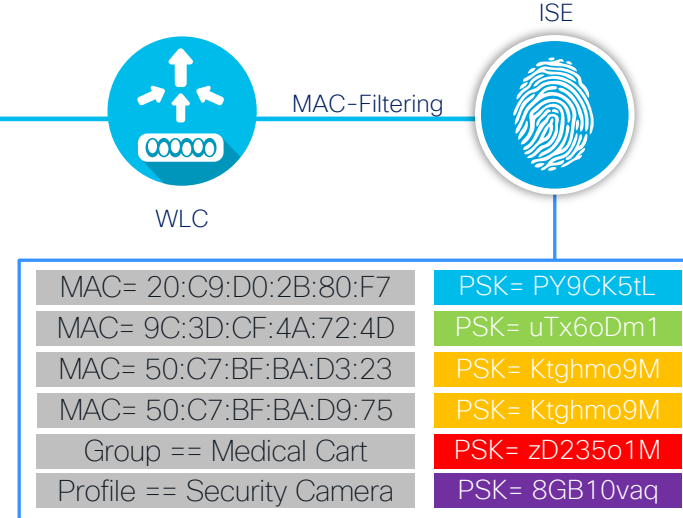
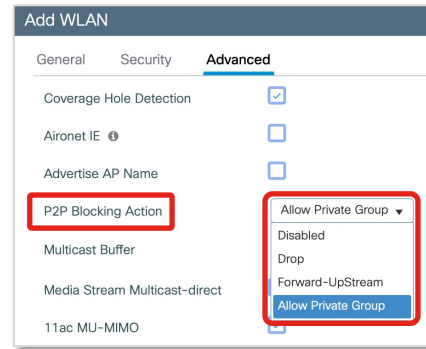
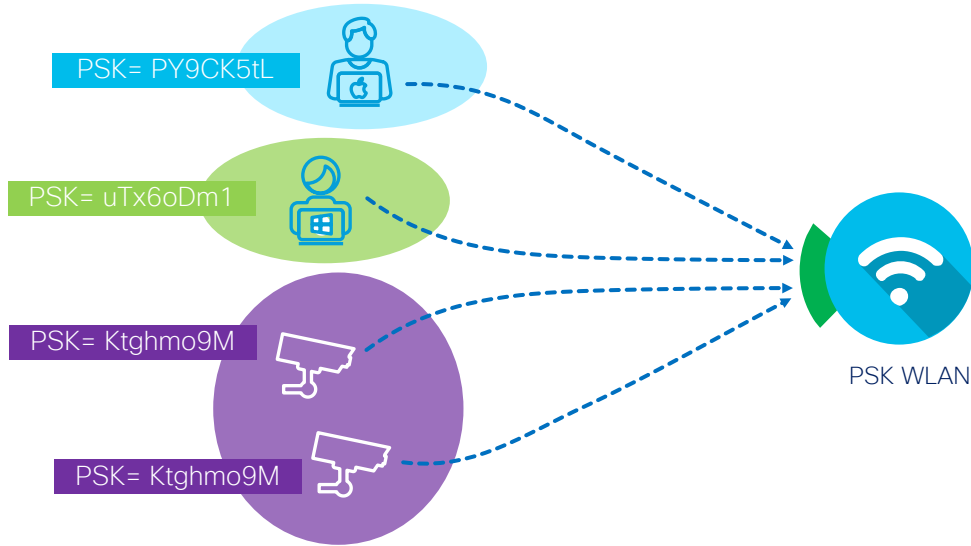
Cancel Apply

Identity PSK



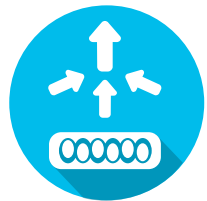
<https://www.cisco.com/c/en/us/support/docs/wireless/catalyst-9800-series-wireless-controllers/216130-configure-catalyst-9800-wlc-ipsk-with-ci.html>
https://documentation.meraki.com/MR/Encryption_and_Authentication/IPSK_with_RADIUS_Authentication

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

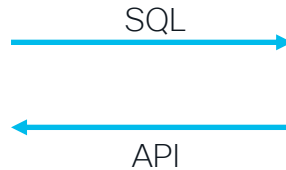
iPSK Manager



WLC / AP

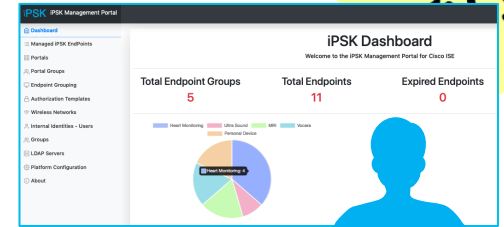


ISE



iPSK Manager

- Linux
- Apache
- MySQL
- PHP



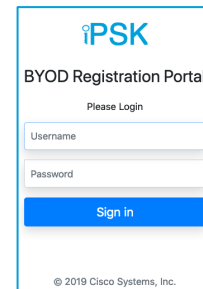
Admin

Administration

iPSK Lifecycle Management



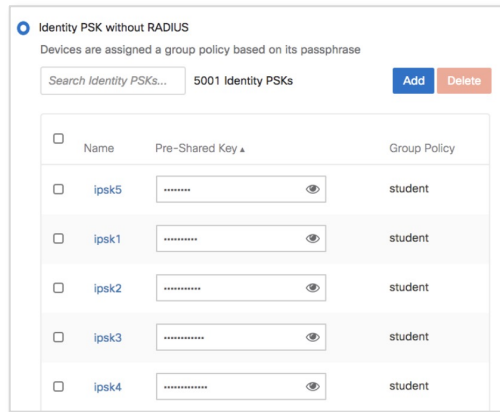
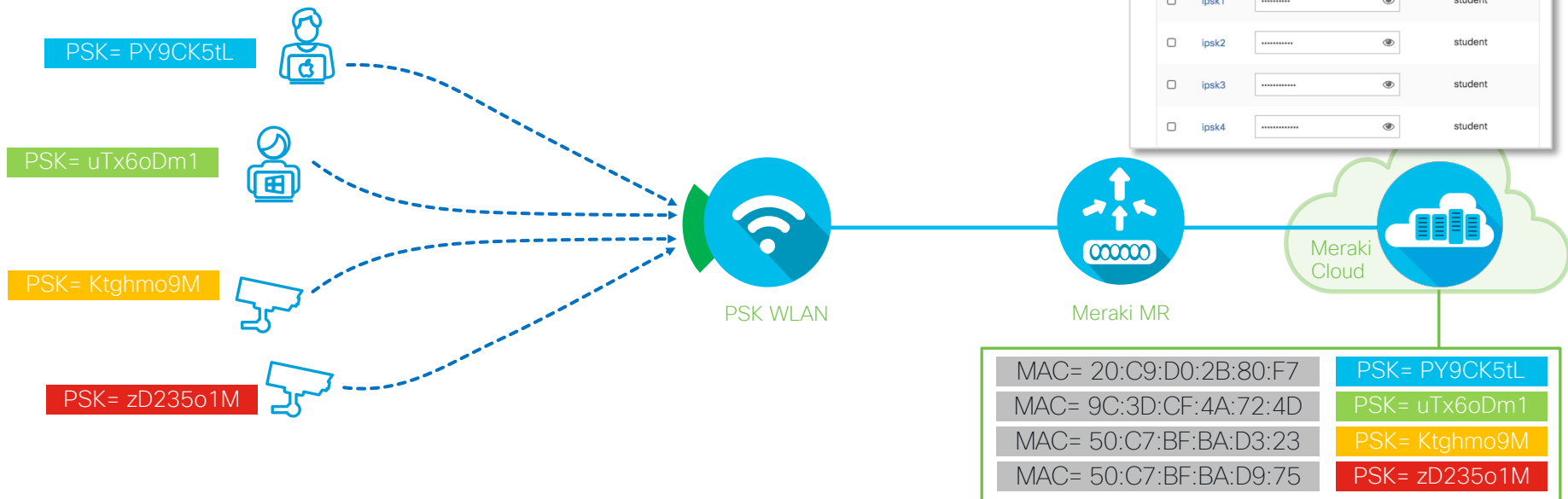
End Users



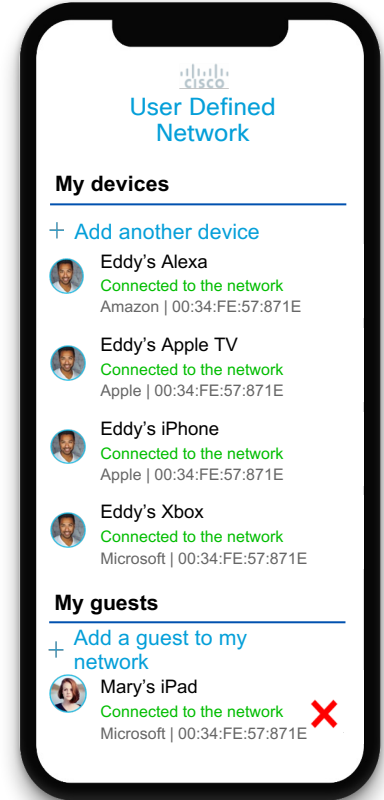
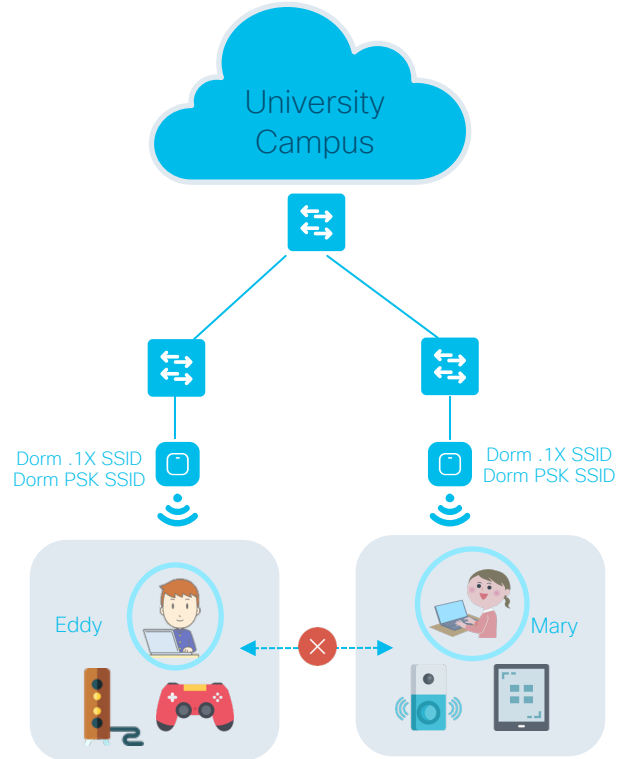
<http://cs.co/iPSK-Manager>

CISCO Live!

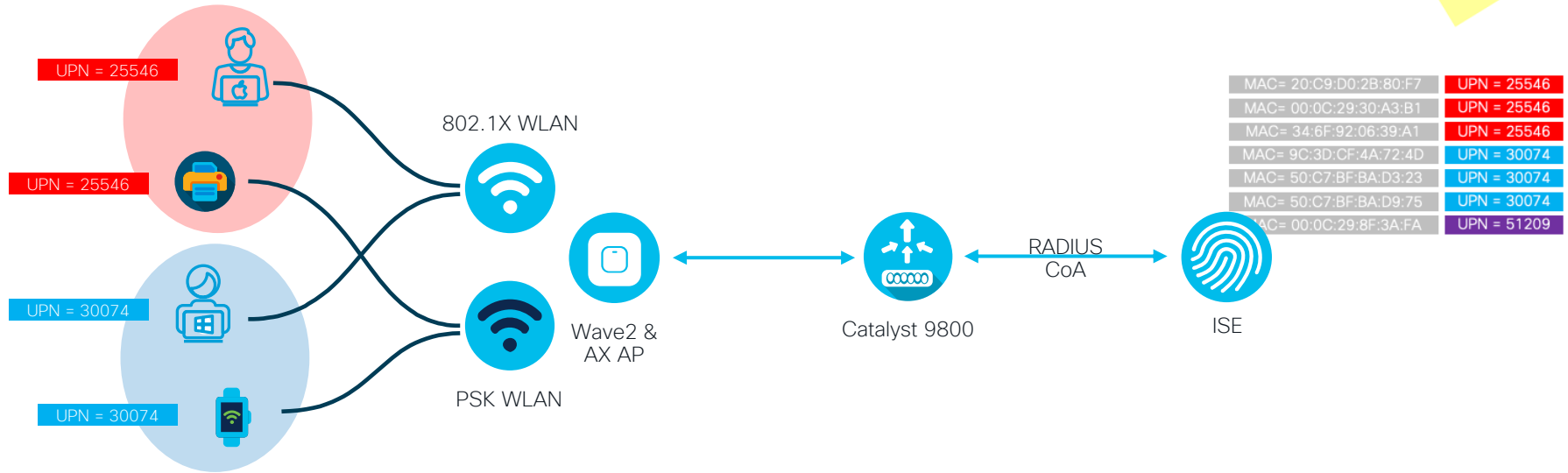
Identity PSK without RADIUS



User Defined Network

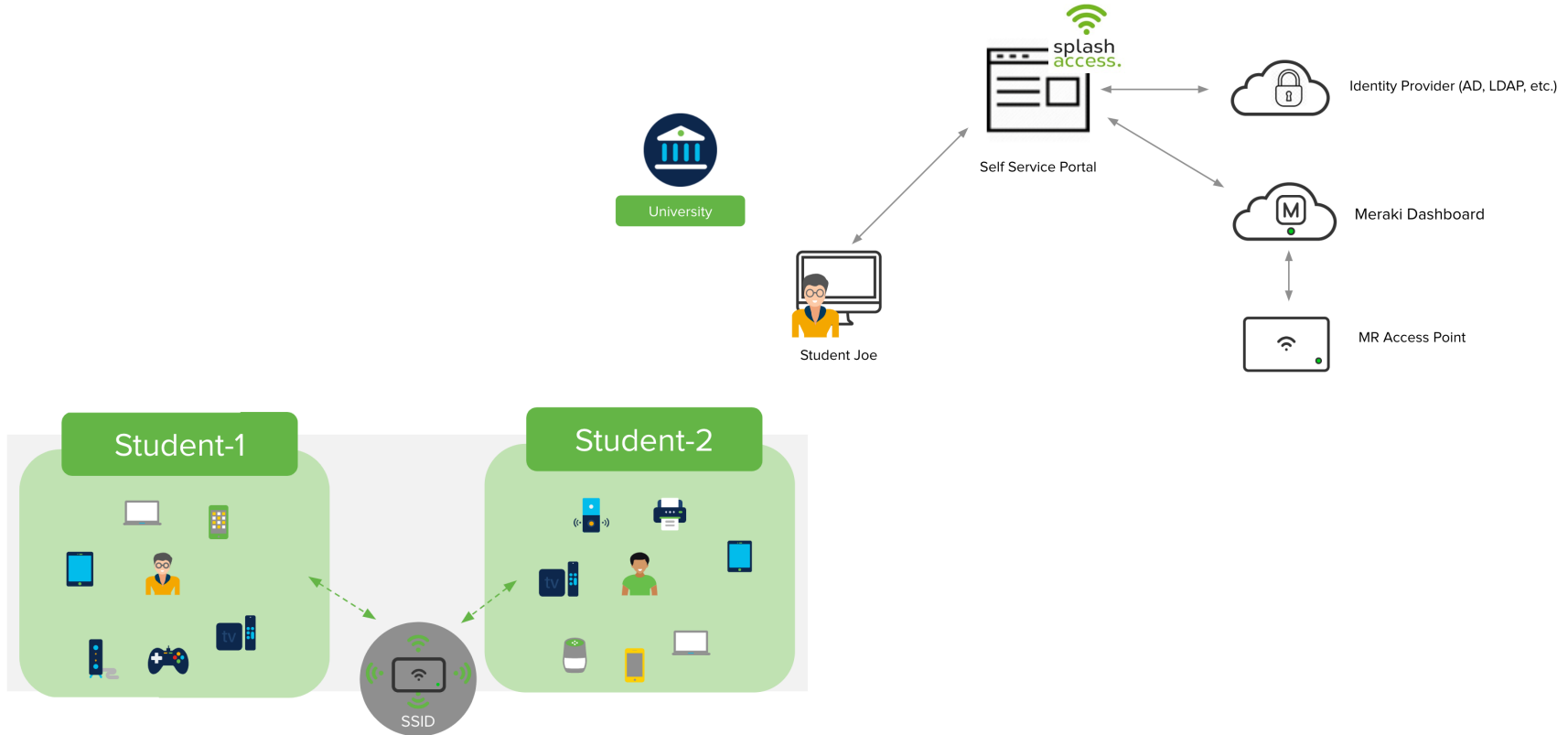


User Defined Network



- Each endpoint is assigned a UPN value via RADIUS
- Works across multiple WLANs and WLAN types
- Endpoint without UPN mapping gets UPN ID of 0
- Filtering can be for mDNS only or for any traffic

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

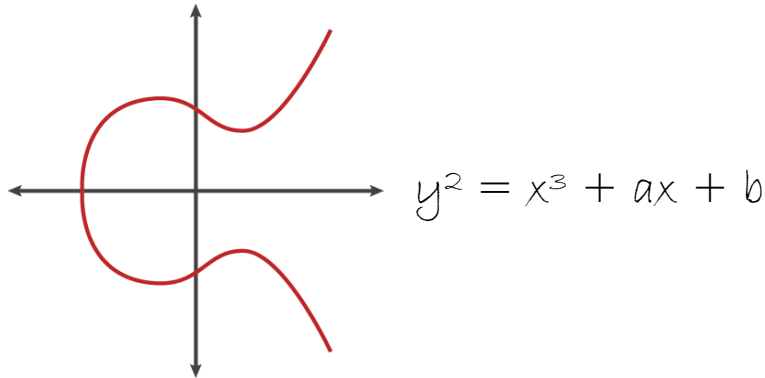
Dragonblood

- 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

The screenshot shows the 'Edit WLAN' configuration page for a WLAN. The 'Security' tab is selected, and the 'Layer2' section is active. The security mode is set to 'WPA3'. The 'Transition Disable' checkbox is checked and highlighted with a red box. Other settings include MAC Filtering (checked), Authorization List (ipsk), WPA Parameters (WPA2 Policy unchecked, WPA3 Policy checked, Transition Disable checked), WPA2/WPA3 Encryption (AES/CCMP128 checked), Protected Management Frame (PMF Required), and Fast Transition (Status Disabled, Reassociation Timeout 20). The Auth Key Mgmt section shows SAE checked and FT + SAE unchecked.

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 WPA2 Policy

GTK Randomize WPA3 Policy

Transition Disable

Fast Transition

Status ▾

Over the DS

Reassociation Timeout *

WPA2/WPA3 Encryption

AES(CCMP128) CCMP256

GCMP128 GCMP256

Protected Management Frame

PMF ▾

Association Comeback Timer*

SA Query Time*

Auth Key Mgmt

SAE FT + SAE

OWE FT + 802.1x

802.1x-SHA256

Anti Clogging Threshold*

Max Retries*

Retransmit Timeout*

PSK Format

PSK Type

Pre-Shared Key*

SAE Password Element ⓘ

Wi-Fi Certified Enhanced Open

WPA3

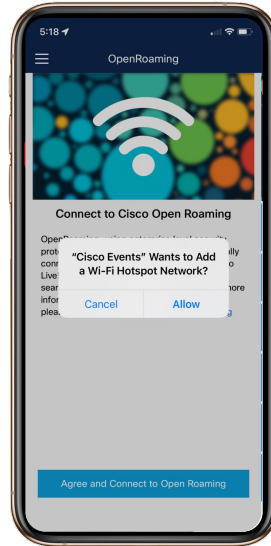
- Opportunistic Wireless Encryption (OWE)
 - Replaces 802.11 “open” authentication support
 - Client and AP perform an unauthenticated Diffie-Hellman Key Exchange to establish a PMK
 - Four-Way Handshake used as normal
 - Supports Protected Management Frames
- Diffie-Hellman is susceptible to MitM attacks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

Decoupling Access and Identity

Access and Identity

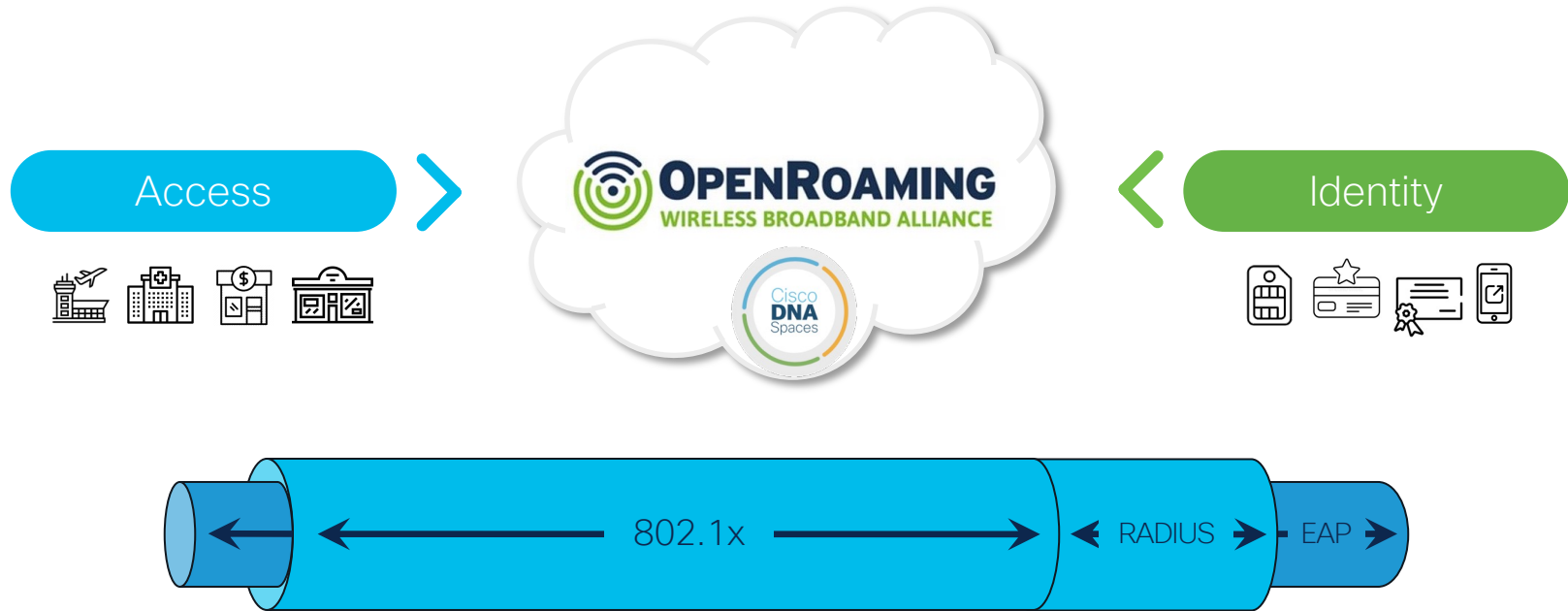
Decoupling Access and Identity

Access



Identity

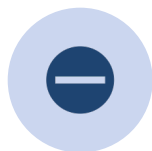
OpenRoaming



Wi-Fi 6E Security



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

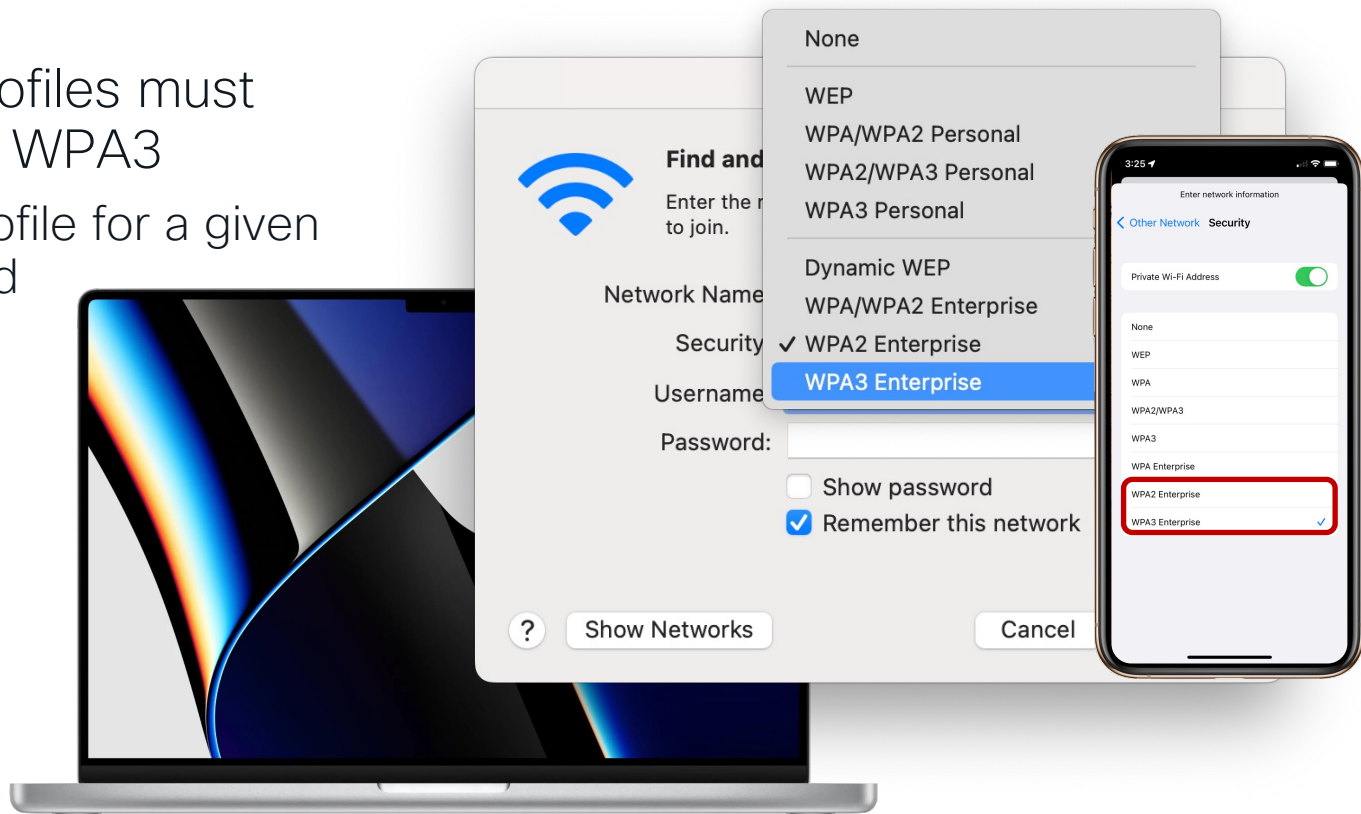


WPA2 and Open are **not** supported on 6GHz

The screenshot displays two overlapping configuration windows for a wireless network profile. The top window is for a profile named 'employee' with SSID 'employee' and radio policy '6 GHz'. The bottom window is for a profile named 'employee-6GHz' with SSID 'employee', WLAN ID '5', and radio policy '6 GHz'. The 6 GHz radio policy is 'ENABLED' with WPA2 Disabled, WPA3 Enabled, and Dot11ax Enabled. The 5 GHz and 2.4 GHz radio policies are 'DISABLED'. The 802.11b/g Policy is set to '802.11g only'.

Wi-Fi 6E 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
- Rogue location and mitigation
- Monitor and classify threats
- Event correlation
- Security compliance reporting

The screenshot displays the Cisco DNA Center Assurance / Dashboards / Rogue and aWIPS interface. The main view is titled 'Threat 360: Mac A4:53:0E:7D:42:A0'. The interface is divided into several sections:

- High Threat Summary:** Shows 135 Active High Threats. A donut chart indicates the distribution: 112 site1rprofile (blue), 12 Rogue on wire (red), and 1 Honey (green).
- Threats (176):** A table listing threats with columns for Threat Level, MAC Address, and Type. The top entries are:

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	Honey
High	A4:53:0E:7D:38:80	Honey
High	A4:53:0E:7D:42:A0	Honey

- Threat 360 View:** Shows details for Threat 360: Mac A4:53:0E:7D:42:A0. It includes a floor plan diagram of the location (Global/San Jose/Building 14/Floor1) with various APs (SJC14-TME-AP1 to AP7) and a central AP (AP-0001). The threat is classified as High, Honeypot, Vendor: Cisco Systems, Inc, Status: Active, Containment Status: Open, and Last Reported: Jun 1, 2022 02:06 pm.
- Detections (18):** A table listing detections with columns for Detecting AP, Detecting AP Site, Adhoc, Rogue SSID, RSSI (dBm), Channels, Radio Type (Band), State, and Last Reported. The top entries are:

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

- Wireless threat detection
- Forensic capture
- Client exclusion policies

The screenshot displays the Cisco Meraki dashboard interface for Wireless Protection Policies. It includes a 'Configuration' breadcrumb, 'Security' and 'Wireless Protection Policies' navigation, and tabs for 'Rogue Policies', 'Rogue AP Rules', and 'Client Exclusion Policies'. A table lists 'Basic Captures (11)' with columns for Alarm ID, Capture Filename, and Last Updated. A modal window titled 'aWIPS and Forensic Capture Enablement' shows options to 'Enable aWIPS' and 'Enable Forensic Capture'. A 'High Threats Summary' section features a donut chart for 'Active High Threats (99)' and a table of threat types such as 'AP Impersonation', 'Association Flood', and 'Fuzzed Beacon'.

Threat Type	Severity	Action	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

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 Pro Dedicated Scanning Radio

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

Configuration > Radio Configurations > CleanAir

5 GHz Band 2.4 GHz Band

General Trap Configuration

Enable CleanAir

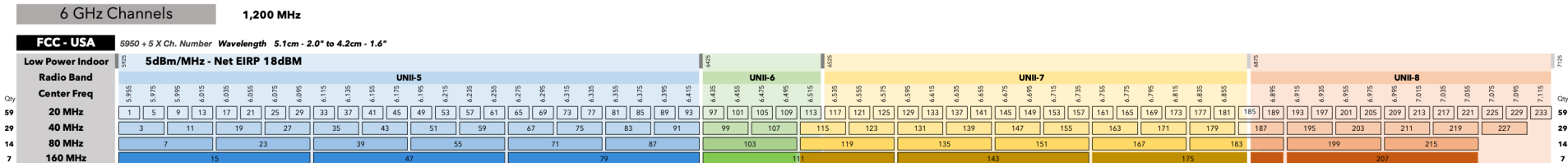
Enable SI

Report Interferers

Available Interference Types Interference Types to detect

WiFi Inverted
WiFi Invalid Channel

TDD Transmitter
Jammer
Continuous Transmitter
DECT-like Phone



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 displays the 'Add AP Join Profile' configuration window, specifically the 'Security' tab. The 'Rogues' section is visible, with 'Rogue Detection' checked. Below this, the 'Rogue Policies' section is expanded, showing 'Rogue AP Rules' selected. The 'Detect and Report Adhoc Networks' checkbox is checked and highlighted with a red box. Other settings include 'Rogue Detection Security Level' set to 'Custom', 'Expiration timeout for Rogue APs' at 1200 seconds, 'Rogue Polling Interval' at 3600 seconds, and 'Rogue Detection Client Number Threshold' at 0. The 'Auto Contain' section is also visible, with 'Auto Containment Level' set to 1. The 'MFP Configuration' section shows 'Global MFP State' and 'AP Impersonation Detection' as unchecked, and 'MFP Key Refresh Interval' at 24 hours.

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 **Auto Contain** Apply

Rogue Detection Security Level	Custom	Auto Containment Level	1
Expiration timeout for Rogue APs (seconds)*	1200	Auto Containment only for Monitor Mode APs	<input type="checkbox"/>
Validate Rogue Clients against AAA	<input type="checkbox"/>	Using our SSID	<input type="checkbox"/>
Validate Rogue APs against AAA	<input type="checkbox"/>	Valid client on Rogue AP	<input type="checkbox"/>
Rogue Polling Interval (seconds)	3600	Adhoc Rogue AP	<input type="checkbox"/>
Detect and Report Adhoc Networks	<input checked="" type="checkbox"/>	MFP Configuration	
Rogue Detection Client Number Threshold*	0	Global MFP State	<input type="checkbox"/>
Rogue Init Timer (seconds)*	180	AP Impersonation Detection	<input type="checkbox"/>
AP Authentication	<input type="checkbox"/>	MFP Key Refresh Interval (hours)*	24
AP Authentication Alarm Threshold*	1		
Syslog Notification	<input type="checkbox"/>		

DNA Center Threat Levels

Informational

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

Potential

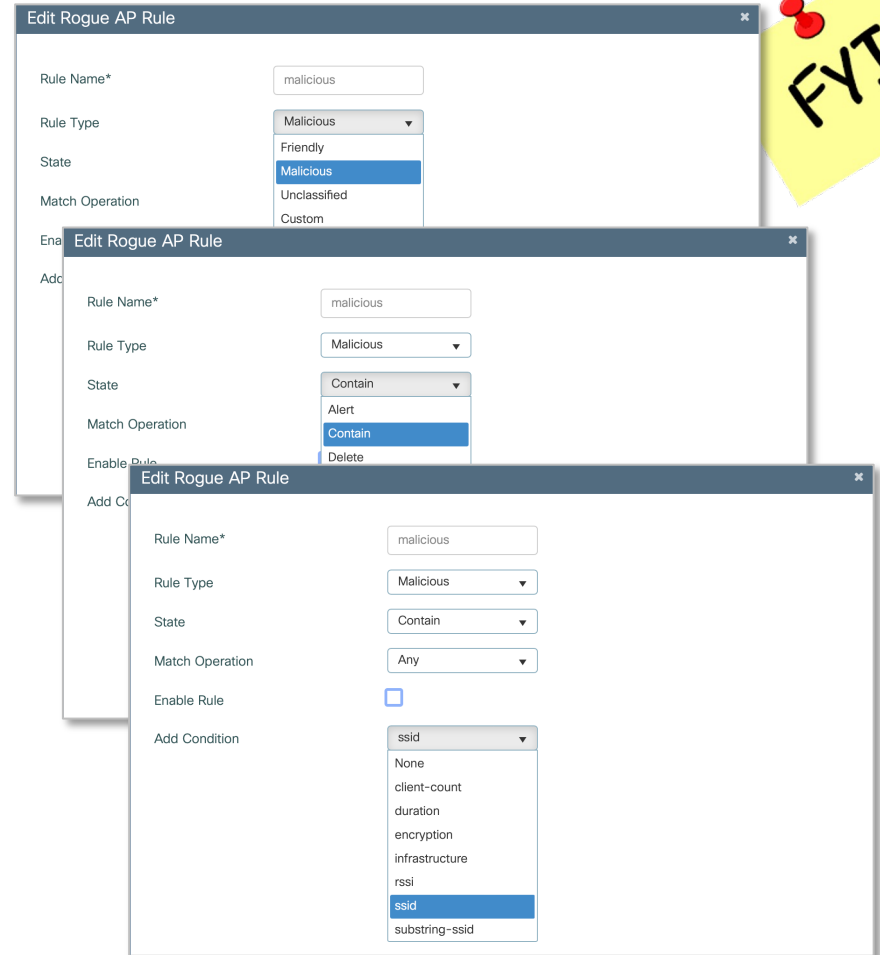
- RSSI $>$ -75 dBm and not on wire
- Rogue Type: Interferer

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



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 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. The main view shows a threat entry for 'Threat 360: Mac A4:53:0E:7C:99:E0' with a 'High Threat' level. A table lists threat details:

Threat Level	Threat Type	Vendor	Status	Containment S...
High	Honeypot	Cisco Systems, Inc	Active	Open

Below the table is a floor plan of 'Global/San Jose/Building 14/Floor1' showing the location of 'SJC14-TME-AP9'. An 'Actions' menu is open, highlighting 'Start Containment'.

A second window shows another threat entry: 'Threat 360: Mac C6:9E:38:75:52:D8' with a 'Potential' threat level. Its details are:

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

This window also shows a floor plan with 'SJC14-TME-AP2' highlighted in red, indicating its physical location.

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

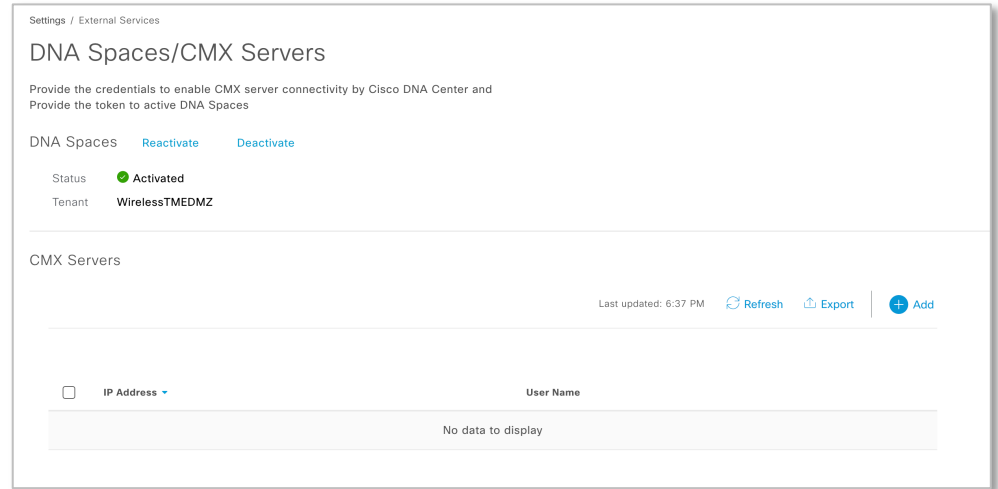
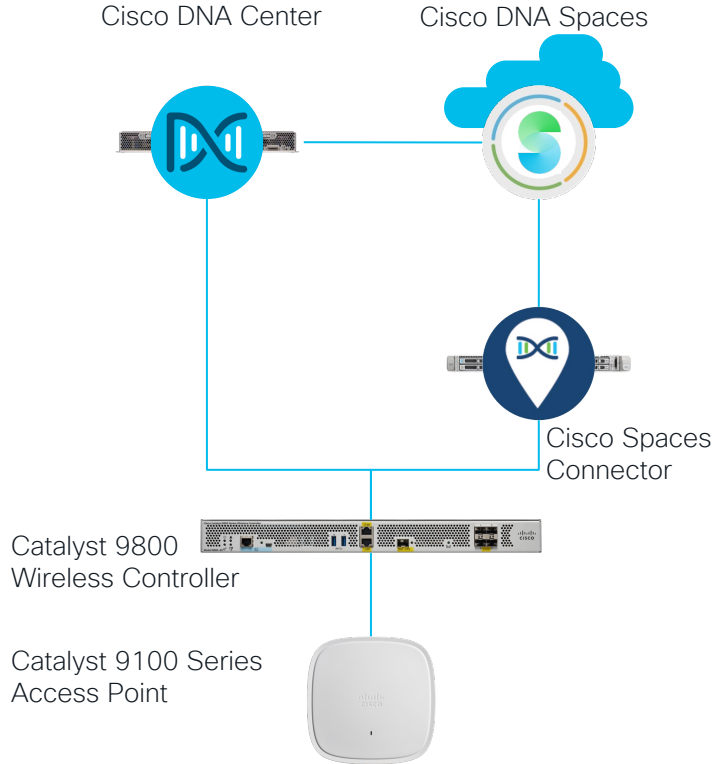
Configuration > Security > Wireless Protection Policies

Rogue Policies Rogue AP Rules Client Exclusion Policies

General **Auto Contain** Apply

Rogue Detection Security Level	Custom	Auto Containment Level	1
Expiration timeout for Rogue APs (seconds)*	1200	Auto Containment only for Monitor Mode APs	<input type="checkbox"/>
Validate Rogue Clients against AAA	<input type="checkbox"/>	Using our SSID	<input type="checkbox"/>
Validate Rogue APs against AAA	<input type="checkbox"/>	Valid client on Rogue AP	<input type="checkbox"/>
Rogue Polling Interval (seconds)	3600	Adhoc Rogue AP	<input type="checkbox"/>
Detect and Report Adhoc Networks	<input checked="" type="checkbox"/>	MFP Configuration	
Rogue Detection Client Number Threshold*	0	Global MFP State	<input type="checkbox"/>
Rogue Init Timer (seconds)*	180	AP Impersonation Detection	<input type="checkbox"/>
AP Authentication	<input type="checkbox"/>	MFP Key Refresh Interval (hours)*	24
AP Authentication Alarm Threshold*	1		
Syslog Notification	<input type="checkbox"/>		

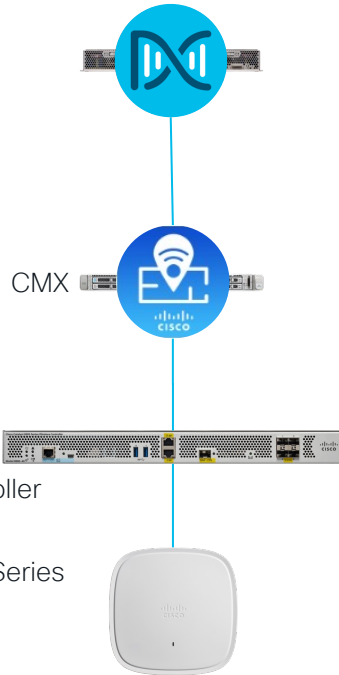
Enabling Location Services



Enabling Location Services



Cisco DNA Center



Settings / External Services

DNA Spaces/CMX Servers

Provide the credentials to enable CMX server connectivity by Cisco DNA Center and Provide the token to active DNA Spaces

DNA Spaces [Reactivate](#) [Deactivate](#)

Status ● **Activated**

Tenant **WirelessTMEDMZ**

CMX Servers

Last updated:

<input type="checkbox"/>	IP Address ▾	User Name
	No data to display	

Add CMX Server

IP Address*

User Name*

Password*

SSH User Name*

SSH Password*

[Cancel](#) [Add](#)

Catalyst 9800
Wireless Controller

Catalyst 9100 Series
Access Point



Rogue on Wire

- Matching Algorithms
 - MAC Address $\pm 2/\pm 1$
 - 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 Assurance dashboard for 'Rogue and aWIPS'. The main view shows a 'Threat 360: Mac 6A:3A:0E:53:A6:E9' with a 'High' threat level and 'Rogue on wire' type. A table lists threat details:

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

Below the table is a floor plan map of 'Global/San Jose/Building 14/Floor1' showing the location of the threat. A table titled 'Switch Port Detail (1)' provides further information:

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

A red box highlights the 'Shutdown Switchport' button in the top right corner of the threat details panel.

Securing AP Switch Port Access



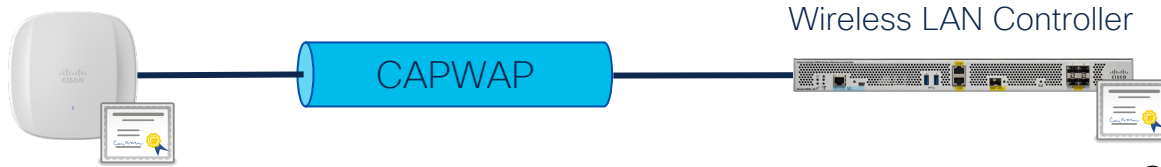
802.1x
Authentication
(EAP-FAST)



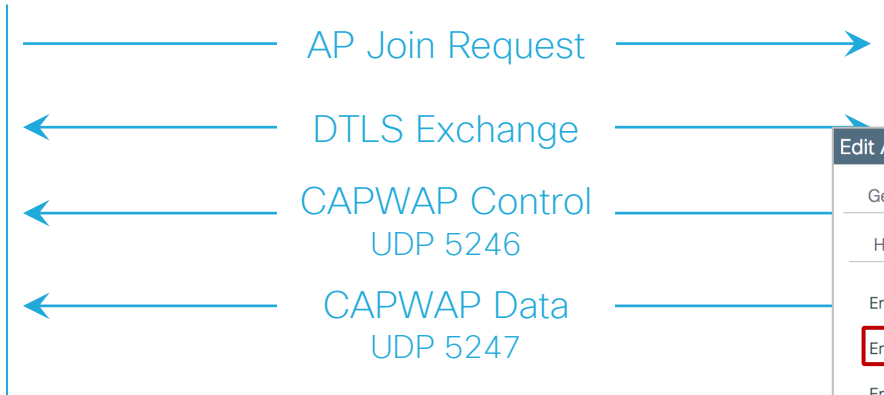
How do we bootstrap configure the AP?

The screenshot shows the 'Add AP Join Profile' configuration window in a network management system. The 'Management' tab is 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



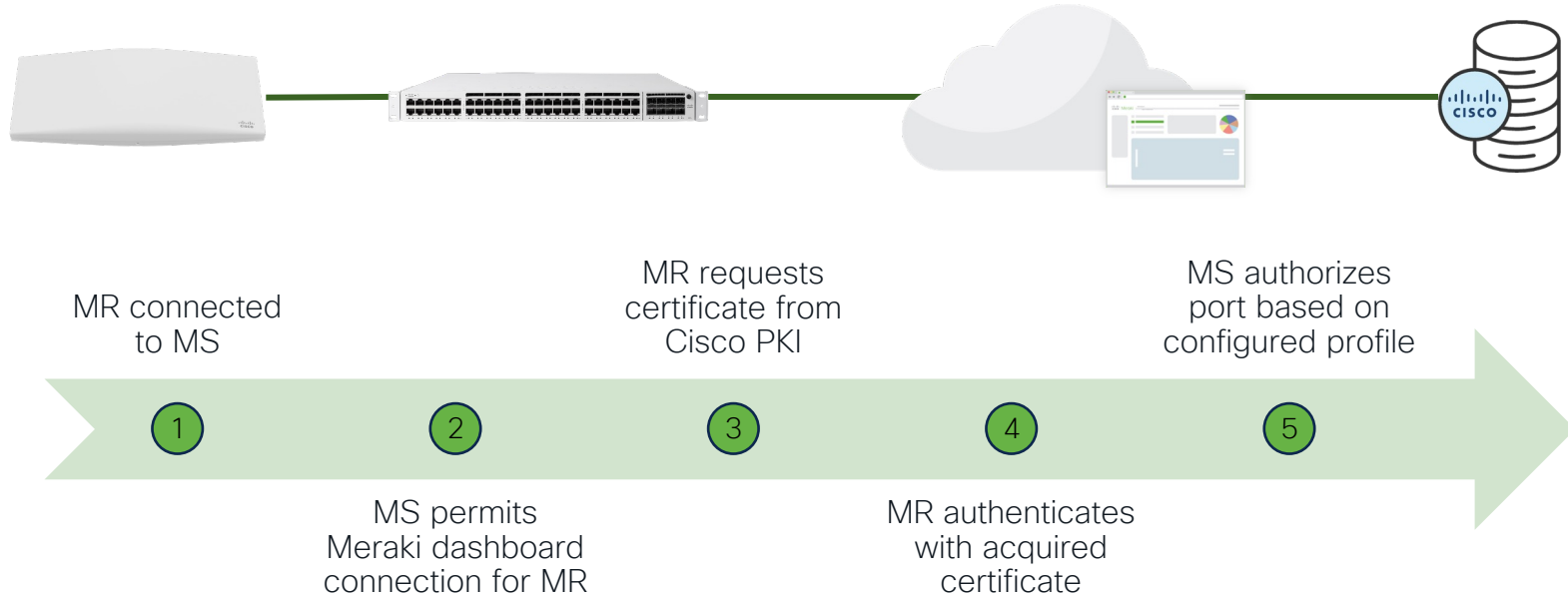
- CAPWAP Control encrypted by default
- CAPWAP Data encapsulated but not encrypted by default



Edit AP Join Profile

General	Client	CAPWAP	AP	Management	Rogue AP
High Availability					
Advanced					
Enable VLAN Tagging	<input type="checkbox"/>				
Enable Data Encryption	<input checked="" type="checkbox"/>				
Enable Jumbo MTU	<input type="checkbox"/>				
Link Latency	Disable				
Preferred Mode	Disable				

SecurePort



Air Marshal

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



Rogue and WIPS Reporting and APIs



The screenshot shows the Cisco DNA Center interface with the 'Reports' section selected. Under 'Report Templates', there are two cards for 'Rogue and aWIPS' reports: 'New Threat' and 'Threat Detail'. Each card includes a brief description, file format options (CSV, TDE, JSON), and a 'Generate' button. The left sidebar shows the navigation menu with 'Rogue and aWIPS' highlighted under 'Network Devices'.

The screenshot shows the Cisco DNA Center Platform / Developer Toolkit interface. The 'APIs' section is active, displaying a list of APIs for 'Rogue and aWIPS'. The table below lists the available APIs:

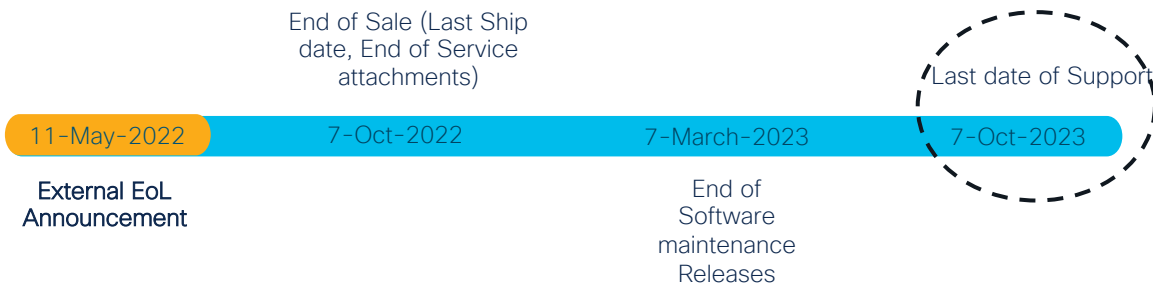
Method	Name	Description	URL	Actions
GET	Get Allowed Mac Address ^{Intent}	Intent API to fetch all the allowed mac addresses in the system.	/security/threats/rogue/allowed-list	...
POST	Threat Summary ^{Intent}	The Threat Summary for the Rogues and aWIPS	/security/threats/summary	...
GET	Get Threat Types ^{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	...

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 would be 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

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	C11111-8P	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

Security Advisories



Cisco DNA Center Tools / Security Advisories

Click [here](#) to access customized security advisories.

ADVISORIES
2 Critical 39 High 28 Medium

SCAN CRITERIA
5 Software Version

Devices (64)
Filter Tag

ADVISORIES
Active Suppressed

Filter 0 Selected Suppress Advisory

Advisory ID	Advisory Title	CVSS Score	Impact	Fixed In
cisco-sa-aaa-Yx47ZT8Q	Cisco IOS XE Software NETCONF and RESTCONF Authentication Bypass Vulnerability	9.8	Critical	16.9.8 16.9.8
cisco-sa-teletd-EFJEzPx	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

Security Advisories



Home / Cisco Security / Security Advisories

Cisco Security Advisory

Cisco IOS XE Software NETCONF and RESTCONF Authentication Bypass Vulnerability

Critical

Advisory ID:	cisco-sa-aaa-Yx47ZT8Q	CVE-2021-1619	Download CVRF
First Published:	2021 September 22 16:00 GMT	CWE-824	Email
Version 1.0:	Final		
Workarounds:	Yes		
Cisco Bug IDs:	CSCv53563		
CVSS Score:	Base 9.8		

Summary

A vulnerability in the authentication, authorization, and accounting (AAA) function of Cisco IOS XE Software could allow an unauthenticated, remote attacker to bypass NETCONF or RESTCONF authentication and do either of the following:

- Install, manipulate, or delete the configuration of an affected device
- Cause memory corruption that results in a denial of service (DoS) on an affected device

This vulnerability is due to an uninitialized variable. An attacker could exploit this vulnerability by sending a series of NETCONF or RESTCONF requests to an affected device. A successful exploit could allow the attacker to use NETCONF or RESTCONF to install, manipulate, or delete the configuration of a network device or to corrupt memory on the device, resulting a DoS.

Cisco has released software updates that address this vulnerability. There are workarounds that address this vulnerability.

Cisco Security Vulnerability Policy

To learn about Cisco security vulnerability disclosure policies and publications, see the [Security Vulnerability Policy](#). This document also contains instructions for obtaining fixed software and receiving security vulnerability information from Cisco.

Subscribe to Cisco Security Notifications

[Subscribe](#)

Related to This Advisory

[Cisco Event Response: September 2021 Semiannual Cisco IOS and IOS XE Software](#)

[Feedback](#)

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](#)

Security Advisories



The screenshot displays the Cisco DNA Center interface for Security Advisories. The main panel shows details for the device `SJC14F1-WTME-C9K-48UXM.cisco.com (172.20.224.109)`, which is `Reachable` with an `Uptime: 25 days 7 hrs 24 mins`. The `Advisories` tab is active, showing a terminal window with the following content:

```
Command Runner SJC14F1-WTME-C9K-48UXM.cisco.com@172.20.224.109
Welcome to Cisco DNA Center command runner.
You can access this window from anywhere using the key combination Q+F.
You can access recently viewed devices using the key combination Q+D.
Note: You can enter "man" anytime to get the list of currently supported commands and shortcuts.
SJC14F1-WTME-C9K-48UXM.cisco.com> show running-config | include aaa authentication login
```

Security Advisories



The screenshot displays the Cisco DNA Center interface. The main header shows 'Cisco DNA Center' and 'Tools / Security Advisories'. A specific device is selected: 'SJC14F1-WTME-C9K-48UXM.cisco.com (172.20.224.109)'. The device status is 'Reachable' with an uptime of '25 days 7 hrs 24 mins'. Below this, there are tabs for 'Details', 'Advisories', and 'Configuration'. The 'Advisories' tab is active, showing a 'Command Runner' window for the selected device. The command runner displays the following text:

```
Welcome to Cisco DNA Center command runner.

You can access this window from anywhere using the key combination Q+T.
You can access recently viewed devices using the key combination Q+D.

Notes: You can enter "man" anytime to get the list of currently supported commands and
shortcuts.

SJC14F1-WTME-C9K-48UXM.cisco.com> show running-config | include aaa authentication 1
ogin
: fetching...
```

On the left side of the interface, there is a sidebar with 'ADVISORIES' showing counts for Critical (2), High (39), and Medium (28). Below that, there are 'Devices' and 'Advisories' sections. The 'SUMMARY' section includes filters for Scan Criteria, Scan Status, Device Family (5), Image Version (16), Sites (48), and Advisory Impact. The 'Devices (64)' section has a list of devices with checkboxes, including 'ASR1K_TME.ASF', 'SJC14F1-WTME', 'c9800-40-TMED', 'SpacesWLC', and 'Spirent_WLC.cis'.

Security Advisories



Cisco DNA Center Tools / Security Advisories

Click [here](#) to access customized security advisories

ADVISORIES
2 Critical 39 High 28 Medium

SCAN CRITERIA
5 Software Version

Devices Advisories

SUMMARY

- > Scan Criteria
- > Scan Status
- > Device Family (5)
- > Image Version (16)
- > Sites (48)
- > Advisory Impact

Devices (64)

Filter Tag

- Device Name
- ASR1K_TME.ASR
- SJC14F1-WTME
- c9800-40-TMED
- SpacesWLC
- Spirent_WLC.cis

SJC14F1-WTME-C9K-48UXM.cisco.com (172.20.224.109)

Reachable Uptime: 25 days 7 hrs 24 mins

Run Commands View 360 Last updated: 3:24 PM Refresh

Details Advisories Configuration

Command Runner SJC14F1-WTME-C9K-48UXM.cisco.com@172.20.224.109

```
Welcome to Cisco DNA Center command runner.

You can access this window from anywhere using the key combination Q+F.
You can access recently viewed devices using the key combination Q+D.

Note: You can enter "man" anytime to get the list of currently supported commands and shortcuts.

SJC14F1-WTME-C9K-48UXM.cisco.com> show running-config | include aaa authentication
login
SJC14F1-WTME-C9K-48UXM.cisco.com>
```

Secure Network Analytics Integration

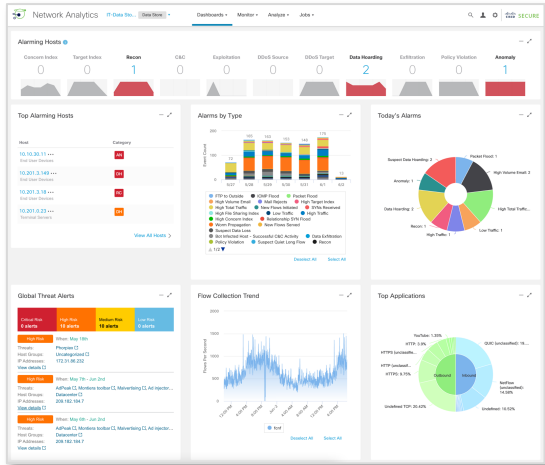
Network as a Sensor



Netflow v9



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	540,000	06/02 3:51:05 PM	10.201.0.15	Atlanta	...
Port Scan - 53	16	172,800	06/02 3:51:05 PM	10.201.0.16	Domain Controllers - Atlanta, DNS Servers	...
Port Scan - 5355	2	21,600	06/02 4:48:45 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

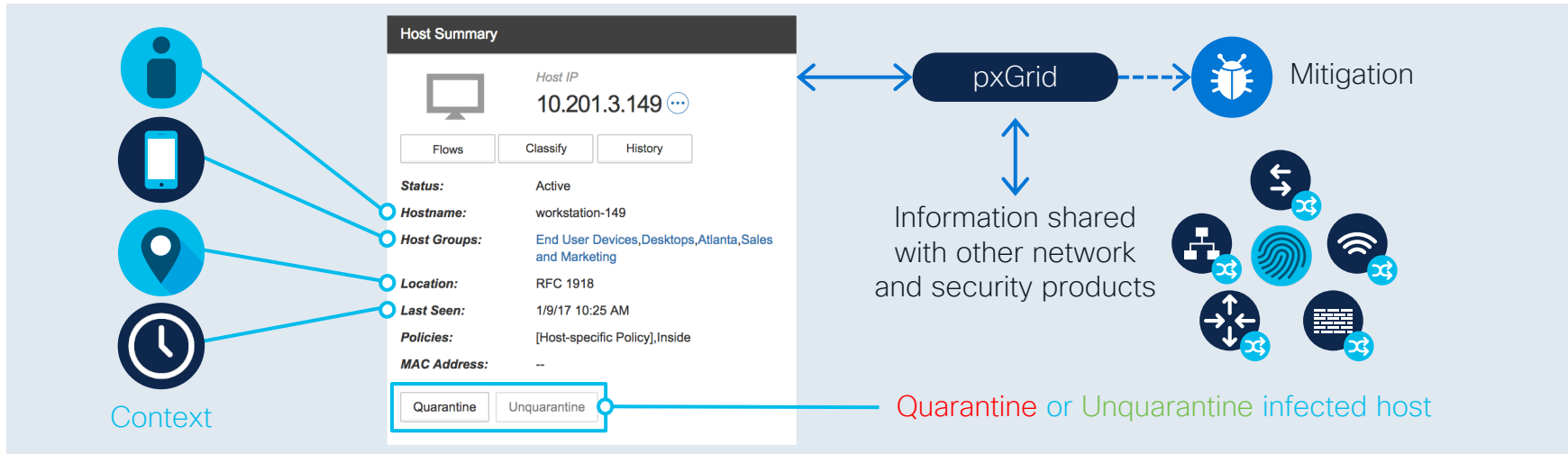
Alert Type Priority
Normal (Default)

[go to alert priorities page](#)



Rapid Threat Containment

Network as an Enforcer

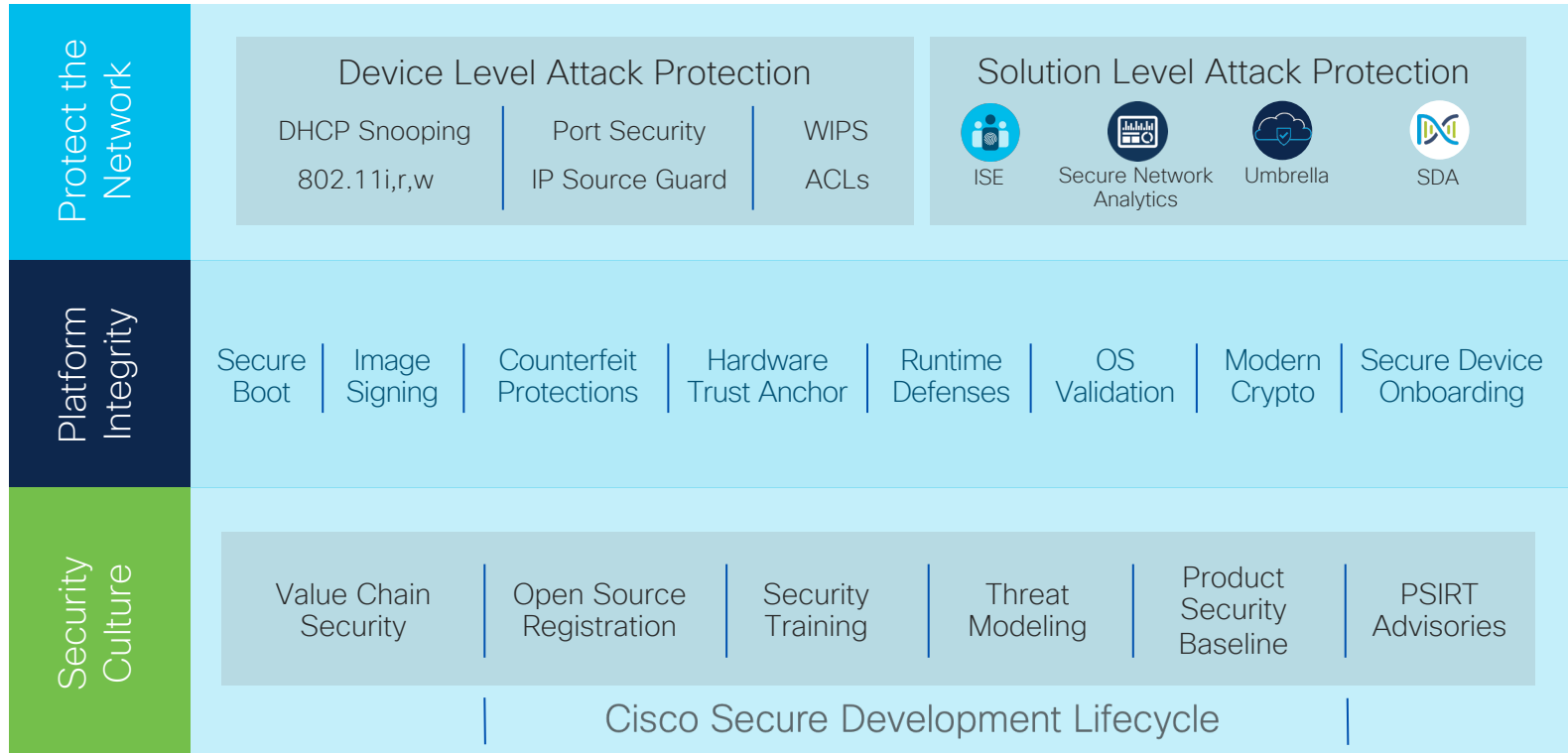


Identity Services Engine



Secure Network Analytics Management Console

Trustworthy Systems



Continue your education



Visit the Cisco Showcase for related demos



Book your one-on-one Meet the Expert 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 Learning and Certifications

From technology training and team development to Cisco certifications and learning plans, let us help you empower your business and career. www.cisco.com/go/certs

Pay for Learning with Cisco Learning Credits

(CLCs) are prepaid training vouchers redeemed directly with Cisco.

Learn

Cisco U.

IT learning hub that guides teams and learners toward their goals

Cisco Digital Learning

Subscription-based product, technology, and certification training

Cisco Modeling Labs

Network simulation platform for design, testing, and troubleshooting

Cisco Learning Network

Resource community portal for certifications and learning

Train

Cisco Training Bootcamps

Intensive team & individual automation and technology training programs

Cisco Learning Partner Program

Authorized training partners supporting Cisco technology and career certifications

Cisco Instructor-led and Virtual Instructor-led training

Accelerated curriculum of product, technology, and certification courses

Certify

Cisco Certifications and Specialist Certifications

Award-winning certification program empowers students and IT Professionals to advance their technical careers

Cisco Guided Study Groups

180-day certification prep program with learning and support

Cisco Continuing Education Program

Recertification training options for Cisco certified individuals

Explore how CX Enterprise Networking Services accelerates outcomes

CX speeds the benefits of an advanced network that predicts, adapts, and protects your business. We offer end-to-end services and guidance to build a future-ready network—all with your unique goals in mind



Visit CX Services for Enterprise Networking to learn more

How we can help

- Future State Architecture
- Architecture and Service Design
- Application, User Experience, and Service Assurance
- Wi-Fi 6/6E Design and Open Roaming
- Software-Defined Access
- Hybrid Cloud
- SD-WAN and Routed Optical Networking
- OT and IOT Secure Networks
- Network Operations and Tools
- Learning
- Certifications

You don't have to do it alone.
For more insight, visit the Cisco CX stand in the World of Solutions for Lightning Talks and Demos

Session Surveys

We would love to know your feedback on this session!

- Complete the session surveys in the Cisco Events mobile app. You'll earn some points in the Cisco Live Game and potentially win a prize.
- Complete a minimum of four session and the overall event surveys to claim a Cisco Live cable bag.



The bridge to possible

Thank you

CISCO *Live!*

#CiscoLiveAPJC

CISCO *Live!*

ALL IN

#CiscoLiveAPJC