
cisco Live!
ALL IN

The bridge to possible

Zero Trust Wireless Access Control

Hosuk Won, Product Manager
@hosukwon
BRKEWN-2462

Cisco Webex App

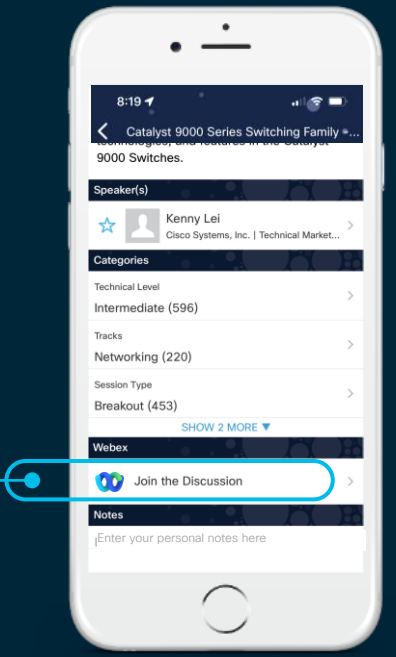
Questions?

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

How

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

Webex spaces will be moderated by the speaker until June 17, 2022.



https://ciscolive.ciscoevents.com/ciscolivebot/#BRKEWN-2462

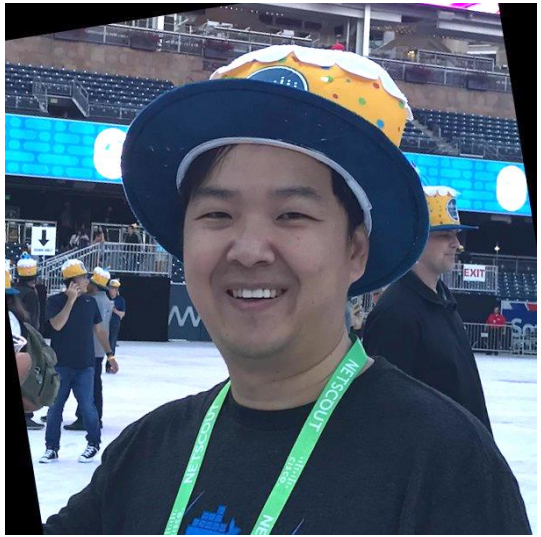
Abstract: BRKEWN-2462

What is the best way to get a user or an endpoint to the network? What are the pros/cons of each EAP (Extensible Authentication Protocol) types? What kind of options are there for IoT wireless access? How can I leverage cloud based identity? If you can't clearly answer these questions for your wireless network, this session is for you. Come and learn ways to securely connect and segment various endpoints to the network.

At the end of this session, participants will learn multiple ways to provide secure access for end users and devices using Cisco wireless solution, ISE (Identity Services Engine), Identity PSK, User Defined Networks micro segmentation, MFA (Multi-Factor Authentication), 802.1X, EAP, SSO (Single-Sign-On), MAB/MAC-Filtering, digital certificates, and web authentication.

About me: Hos(z)uk Won

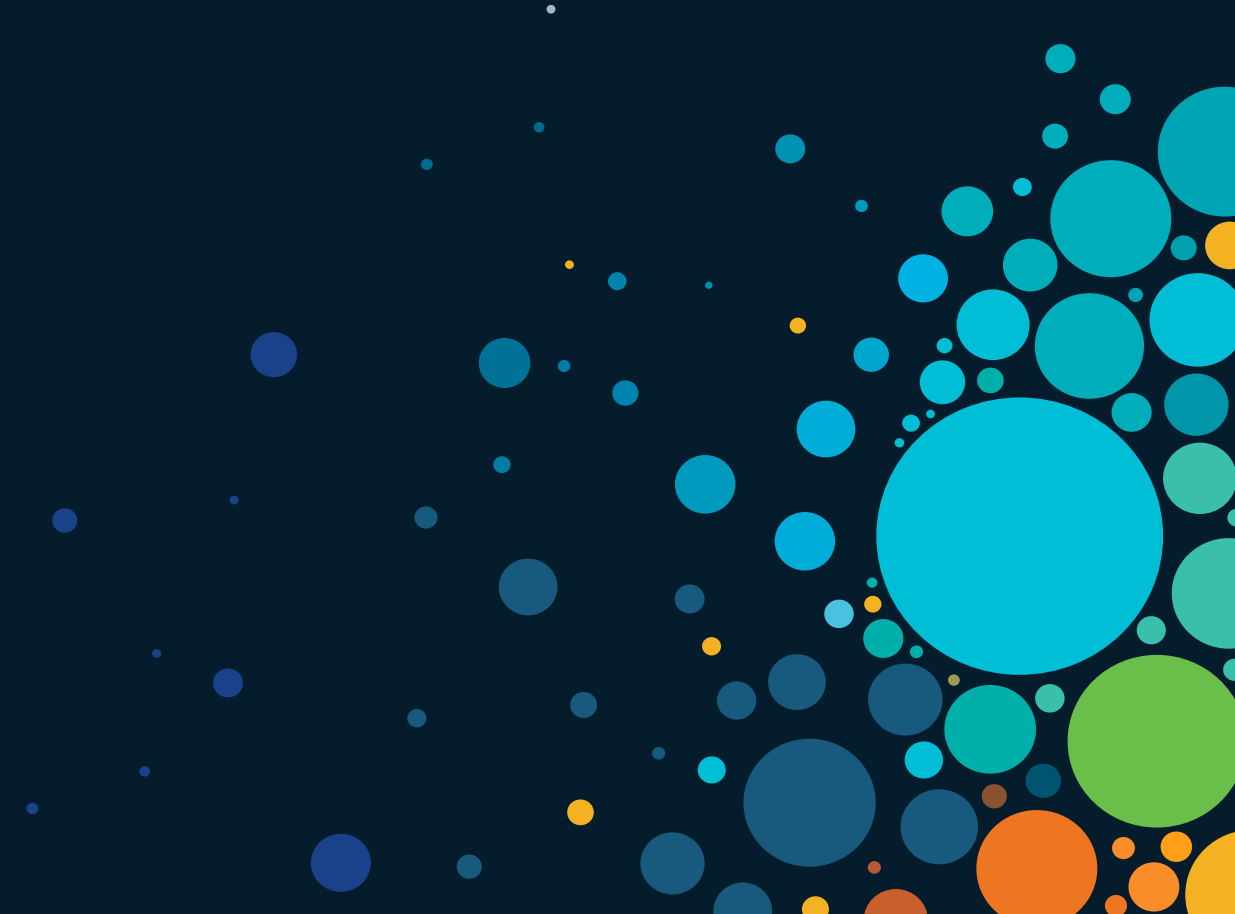
- 17 years with Cisco
  - Currently Product Manager for the Security, Policy & Access (SPA) team
  - Technical Marketing Engineer for the SPA team
  - Consulting Engineer with the security practice
- 2 x CCIE – Wireless & Security



Agenda

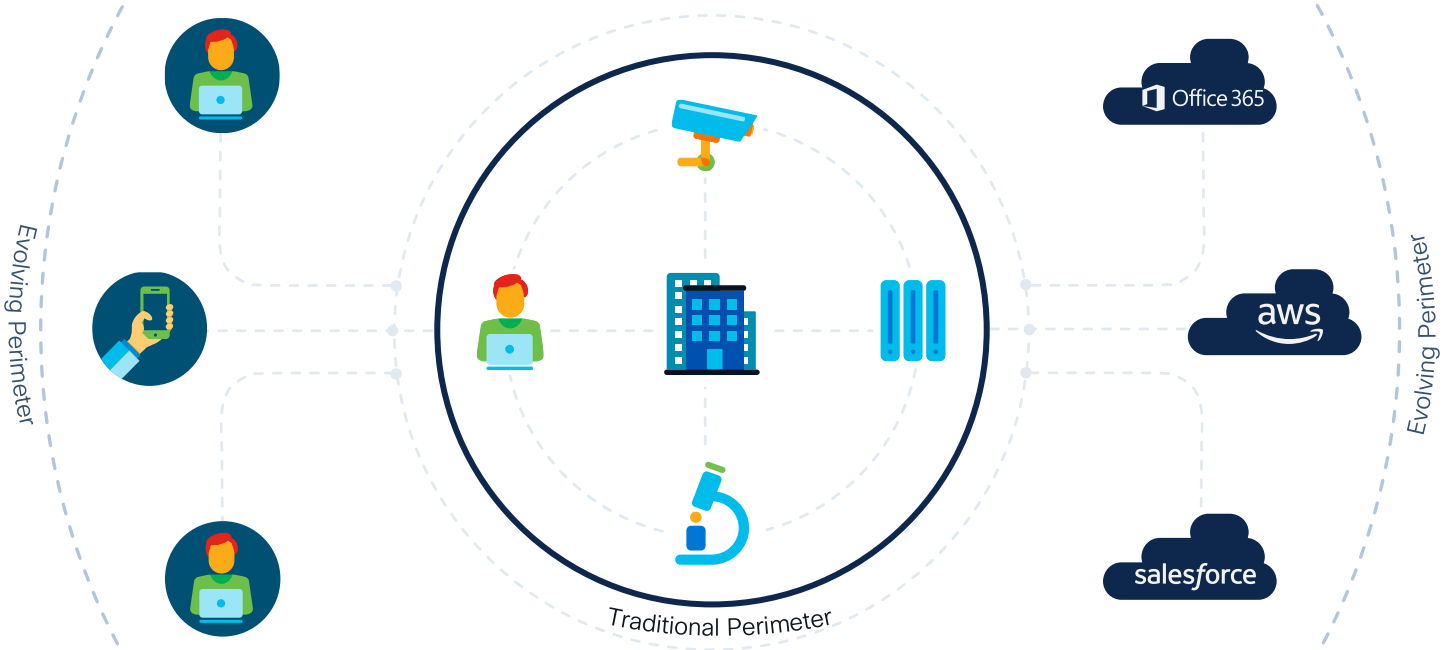
- Introduction
- ZTNA and Wireless
- Wireless authentication
- Access control
- Random MAC address

ZTNA & Wireless



The Enterprise trends

Users, devices and apps are everywhere

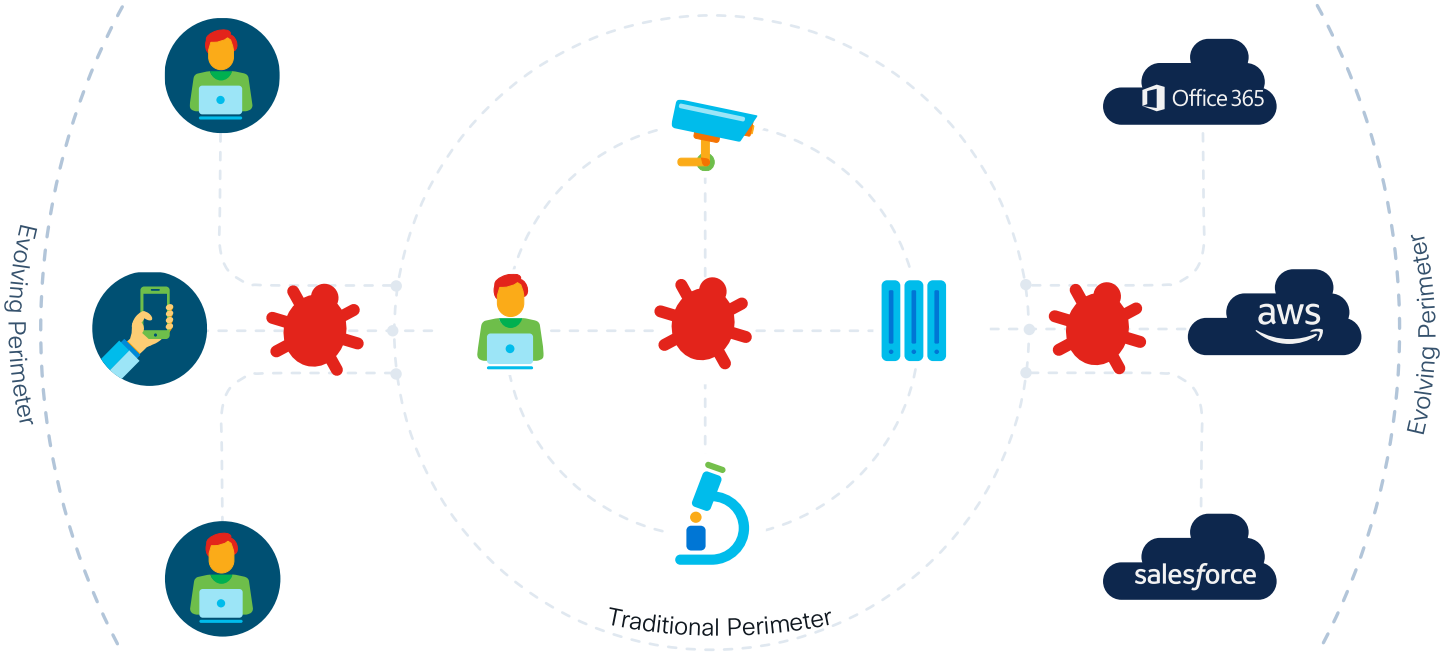


MOBILITY
Increased movement of user-bound devices (within and outside campus)

INTERNET OF THINGS
Proliferation of headless assets with limited security capabilities

CLOUD
Workload movement to multi-cloud. Software consumption via SaaS

Excessive Trust is increasing gaps in visibility and attack surface



Enterprises are enabling data access between
Any User, Any Device, Any App, In Any location.

Moving from excessive trust to “Zero Trust”

A comprehensive approach to securing all access across your networks, applications, and environment.

Workforce

Ensure only the right users and secure devices can access applications.

Workplace

Secure all user and device connections across your network, including IoT.

Workloads

Secure all connections within your apps, across multi-cloud.

Why Zero Trust for Workplace?

	Threats	Zero Trust Solution
1	**Unauthorized endpoints** or devices with unhygienic posture can disrupt productivity	No network access until endpoint trust is evaluated (authenticate and evaluate system health)
2	Noncritical assets with **unrestricted network access** can make the entire infrastructure vulnerable	Provide confined access to essential services through macro and micro-segmentation
3	Compromised endpoints can infect other assets in the network through **lateral movements**	Continuously evaluate trust and apply adaptive controls to isolate threats in the real-time

Zero Trust Network Access – Wireless Workplace

Devices

- Device ecosystem with wireless analytics
- Endpoint Analytics

Air

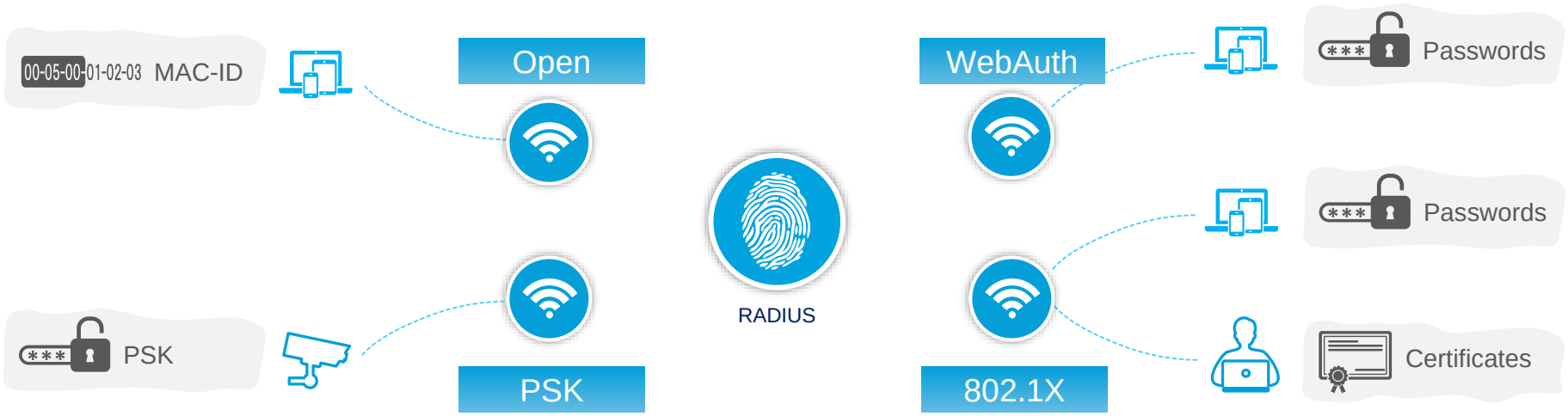
- Automated wireless threat detection & remediation with aWIPS and Rogue AP detection

Network

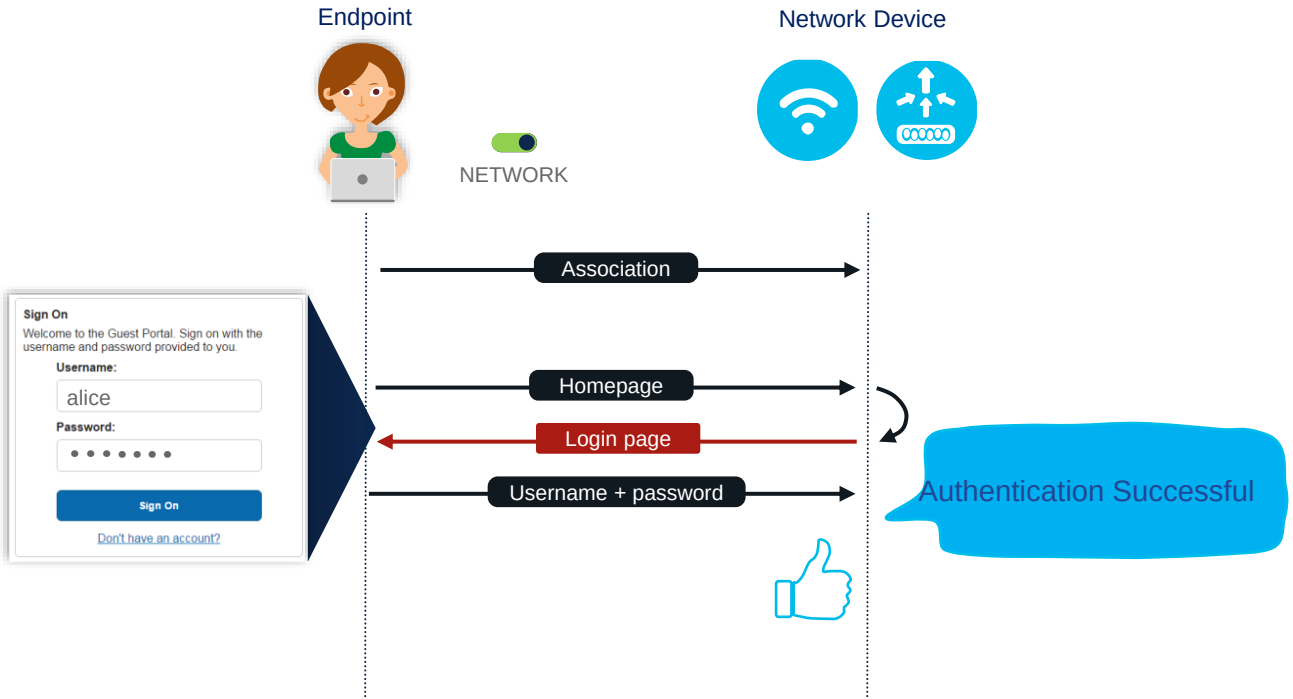
- Wireless authentication
- Macro and Micro segmentation

Wireless Authentication

Wireless LAN Types



Web Authentication (AKA Captive portal)

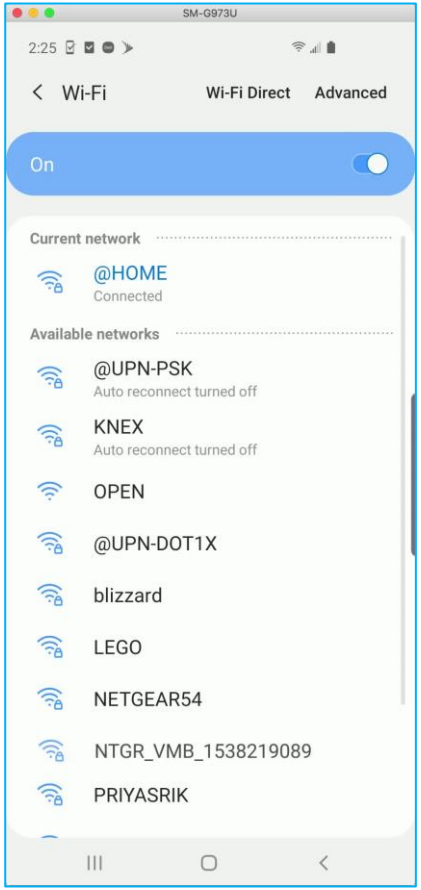


Captive Portal Detection

Windows
- http://www.msftncsi.com/ncsi.txt

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

Apple Devices
- http://captive.apple.com/hotspot-detect.html

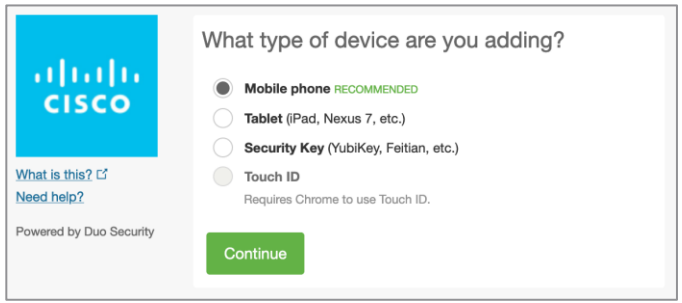


- Nice feature for guest access
- Avoid having to redirect HTTPS traffic
- User is aware of captive portal even when not using browser

Web Authentication + MFA

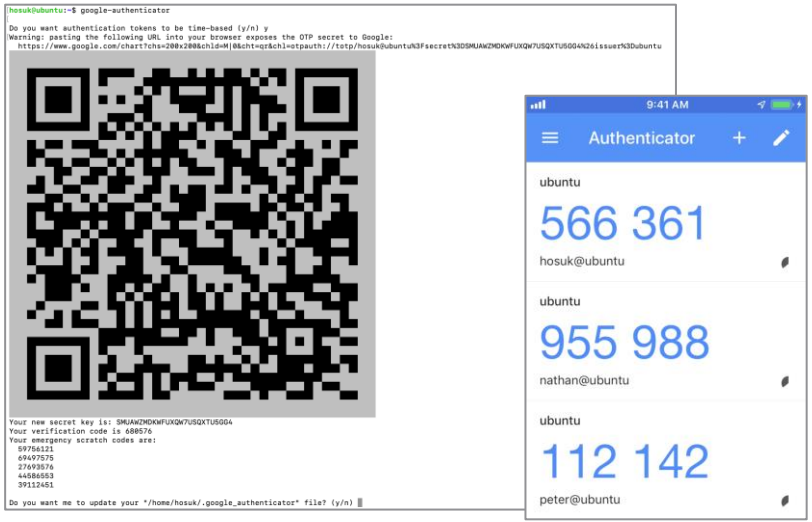
Cisco Duo

- Push is easier for users due to push notification
- Requires Internet

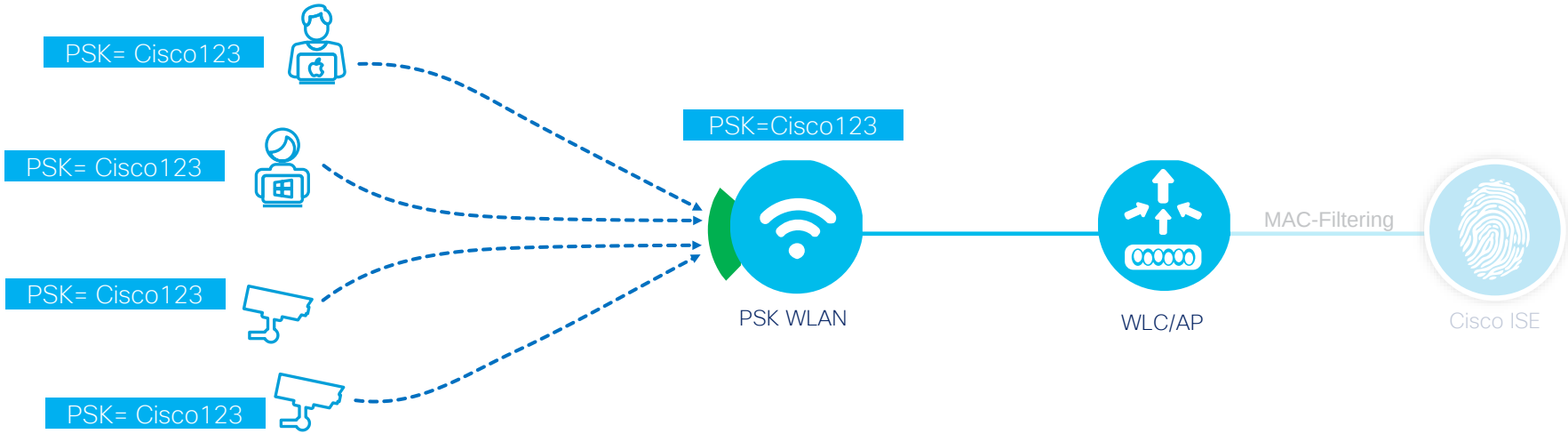


Traditional TOTP

- Free
- User has to open token app manually

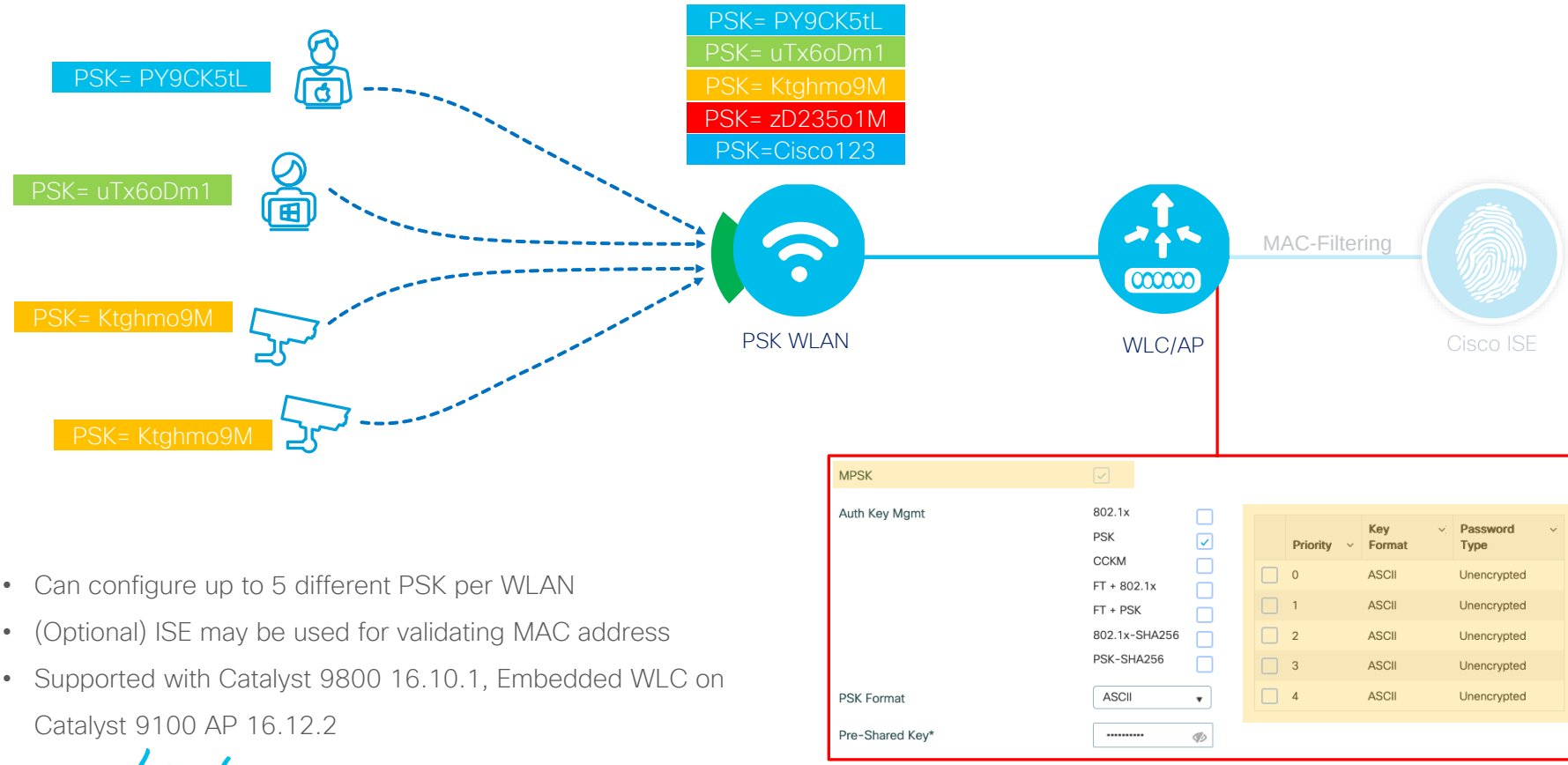


PSK (Pre-Shared Key) WLAN



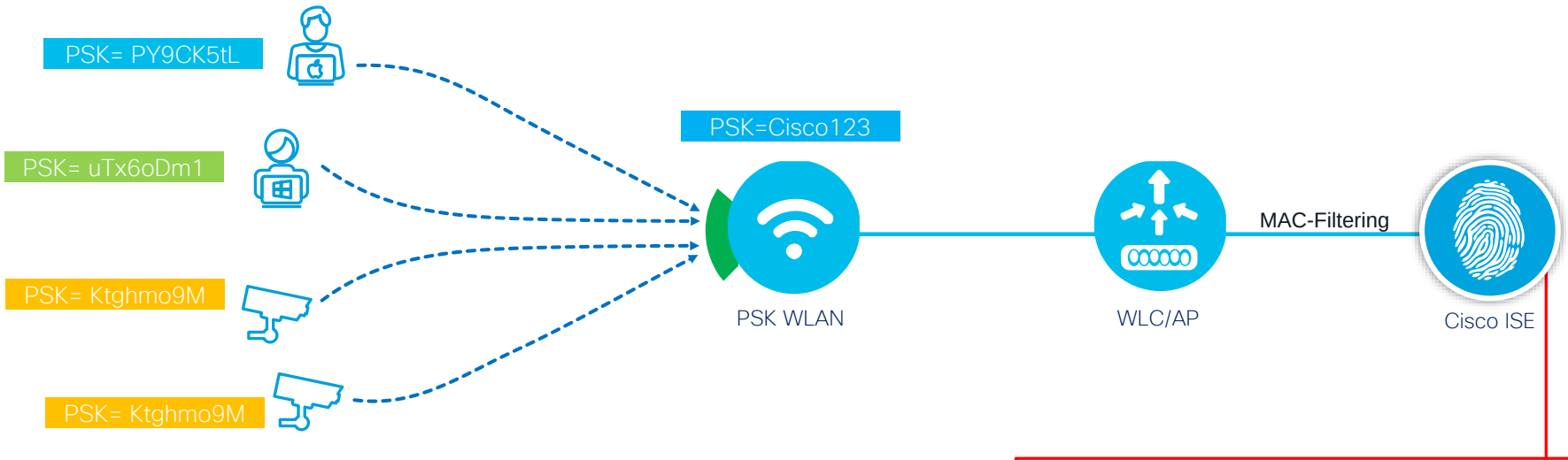
- Each endpoints associate to the single WLAN with same PSK value
- (Optional) ISE may be used for validating MAC address
- Supported on virtually any wireless product

MPSK (Multi PSK)



- Can configure up to 5 different PSK per WLAN
- (Optional) ISE may be used for validating MAC address
- Supported with Catalyst 9800 16.10.1, Embedded WLC on Catalyst 9100 AP 16.12.2

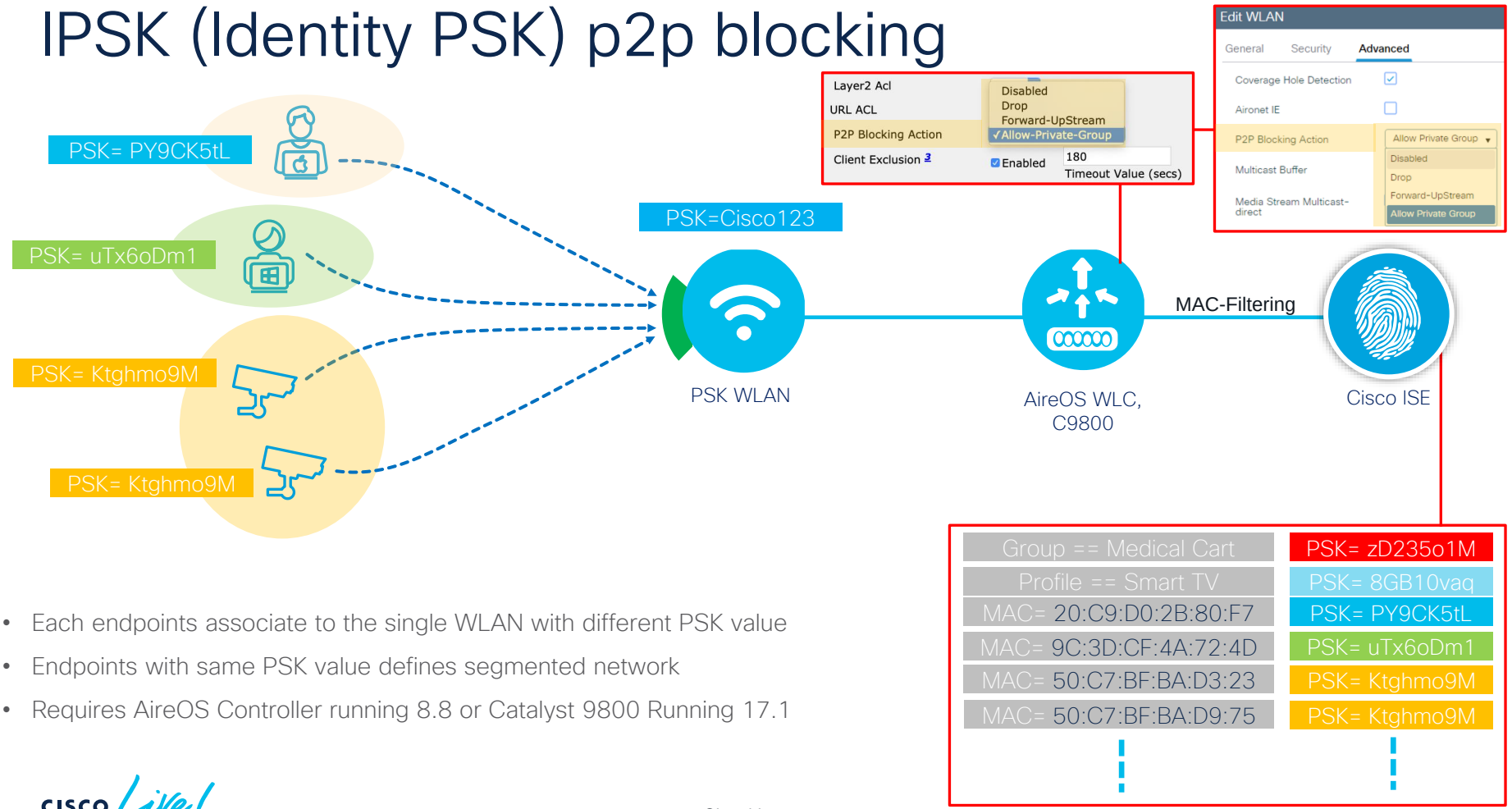
IPSK (Identity PSK)



- Each endpoints associate to the single WLAN with different PSK value
- ISE provides mapping of MAC address to PSK
- Supported with AireOS 8.5, Catalyst 9800 16.10.1, Mobility Express AP 8.8MR2, Embedded WLC on Catalyst 9100 AP 16.12.2, Meraki MR v26

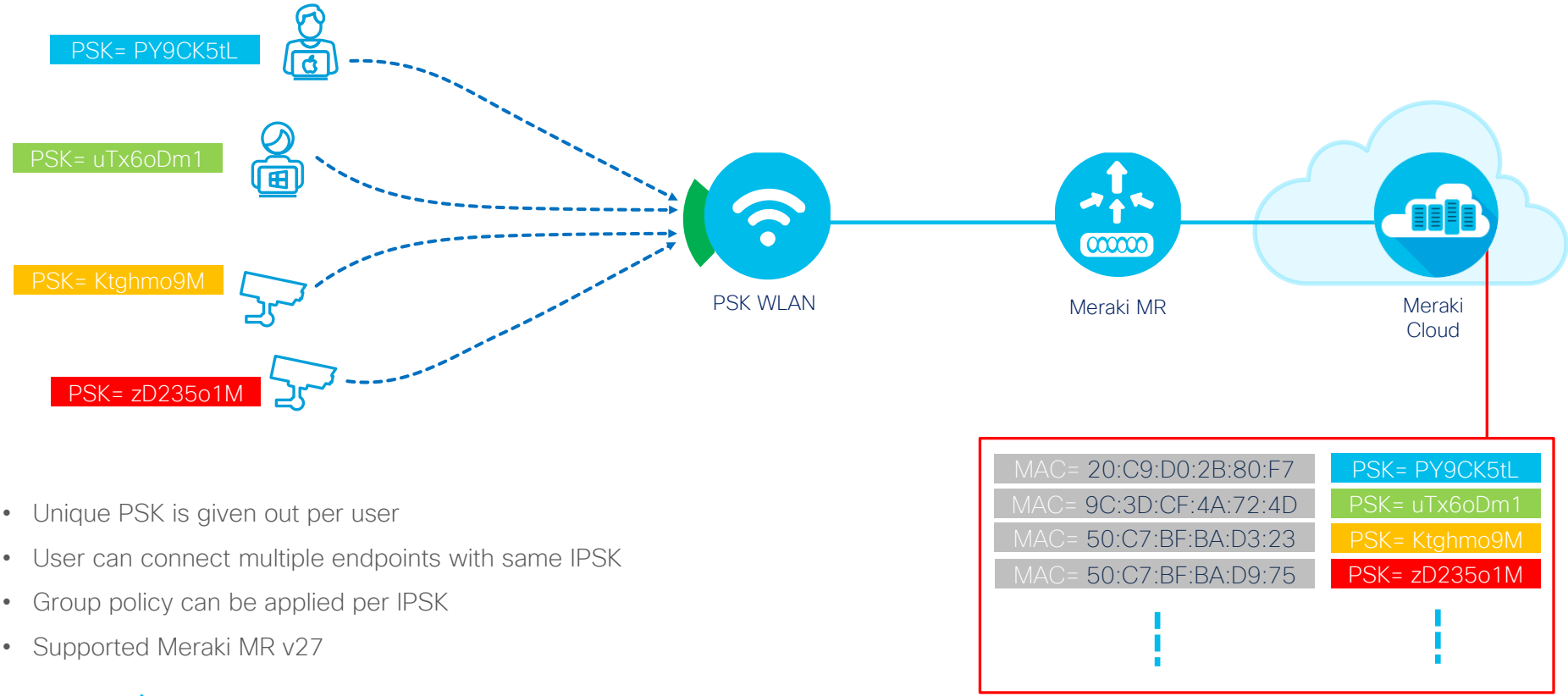
IPSK (Identity PSK) p2p blocking

AireOS | 9800



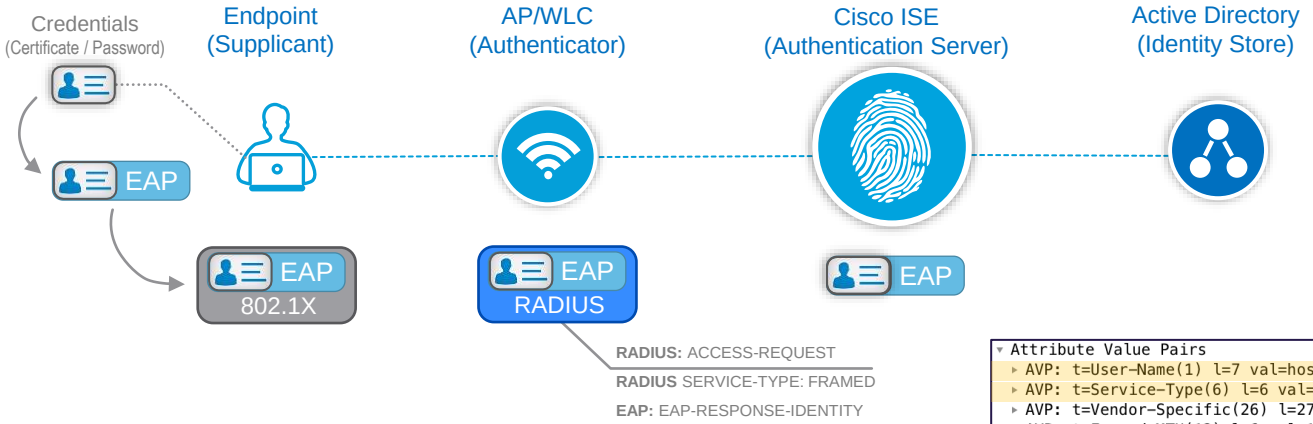
- Each endpoints associate to the single WLAN with different PSK value
- Endpoints with same PSK value defines segmented network
- Requires AireOS Controller running 8.8 or Catalyst 9800 Running 17.1

IPSK without RADIUS



- Unique PSK is given out per user
- User can connect multiple endpoints with same IPSK
- Group policy can be applied per IPSK
- Supported Meraki MR v27

802.1X

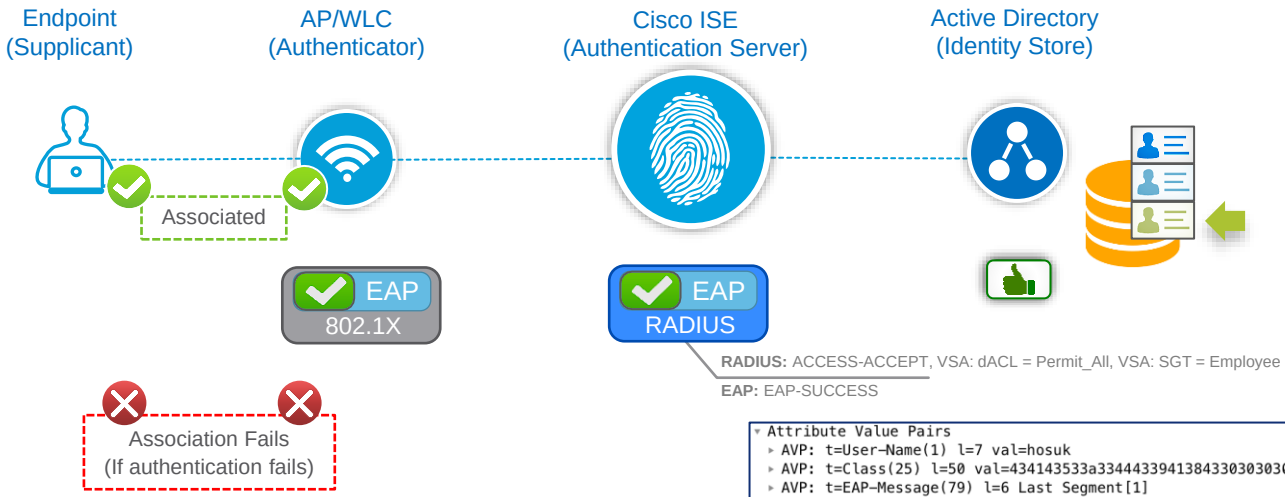


EAP: Extensible Authentication Protocol

Supplicant: Software running on the client that provides credentials to the authenticator (Network Device).

```
▾ Attribute Value Pairs
  ▸ AVP: t=User-Name(1) l=7 val=hosuk
  ▸ AVP: t=Service-Type(6) l=6 val=Framed(2)
  ▸ AVP: t=Vendor-Specific(26) l=27 vnd=ciscoSystems(9)
  ▸ AVP: t=Framed-MTU(12) l=6 val=1485
  ▸ AVP: t=EAP-Message(79) l=12 Last Segment[1]
  ▸ AVP: t=Message-Authenticator(80) l=18 val=10c87be3950f1cec07ae61f4dfad789a
  ▸ AVP: t=EAP-Key-Name(102) l=2 val=
  ▸ AVP: t=Vendor-Specific(26) l=49 vnd=ciscoSystems(9)
  ▸ AVP: t=Vendor-Specific(26) l=20 vnd=ciscoSystems(9)
  ▸ AVP: t=Vendor-Specific(26) l=32 vnd=ciscoSystems(9)
  ▸ AVP: t=Vendor-Specific(26) l=18 vnd=ciscoSystems(9)
  ▸ AVP: t=NAS-IP-Address(4) l=6 val=192.168.201.61
  ▸ AVP: t=NAS-Port-Id(87) l=17 val=capwap_90000004
  ▸ AVP: t=NAS-Port-Type(61) l=6 val=Wireless-802.11(19)
  ▸ AVP: t=NAS-Port(5) l=6 val=8013
  ▸ AVP: t=Called-Station-Id(30) l=31 val=38:0e:4d:4a:3b:20:C9800-DOT1X
  ▸ AVP: t=Calling-Station-Id(31) l=19 val=08:e6:89:2d:26:4d
  ▸ AVP: t=Vendor-Specific(26) l=12 vnd=Airespace, Inc(14179)
  ▸ AVP: t=Vendor-Specific(26) l=35 vnd=ciscoSystems(9)
  ▸ AVP: t=NAS-Identifier(32) l=10 val=C9800-CL
```

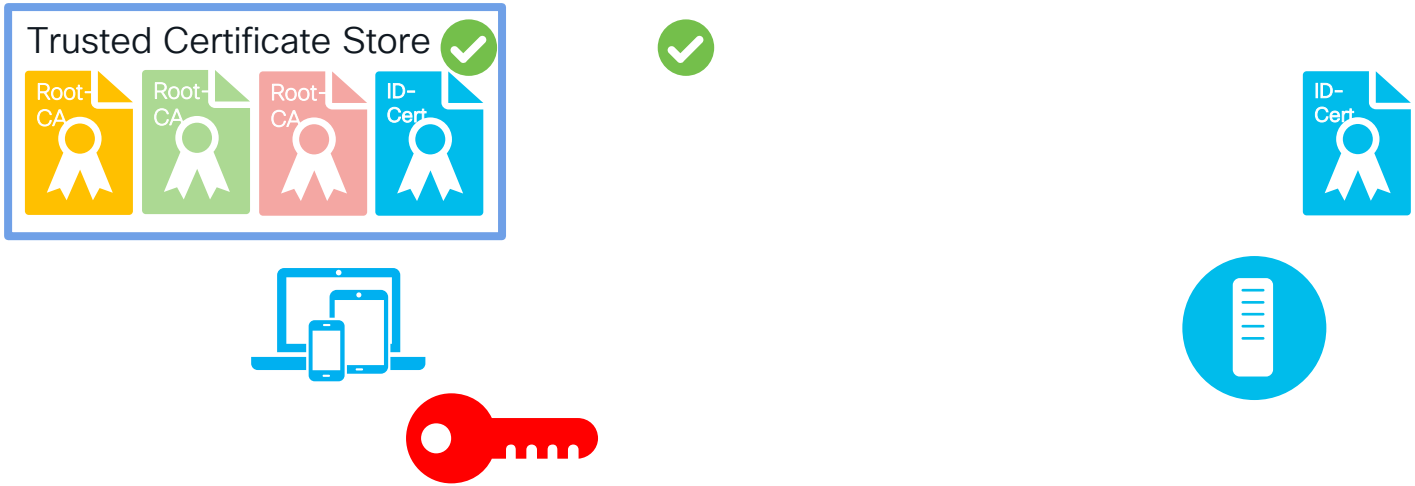
802.1X



Supplicant: Software running on the client that provides credentials to the authenticator (Network Device).

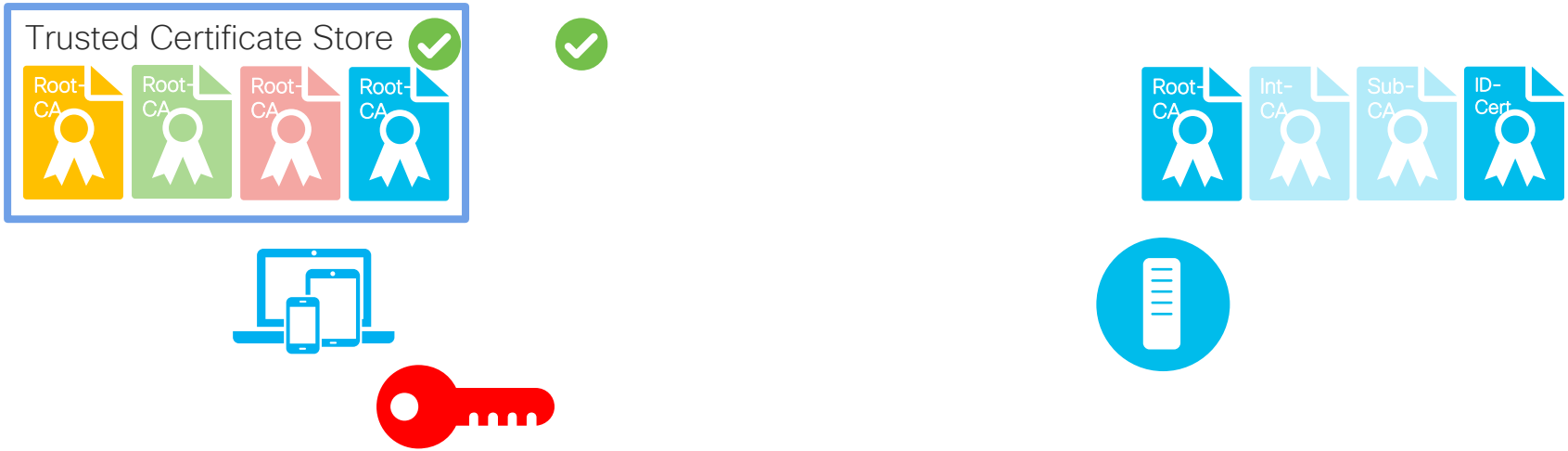
```
▾ Attribute Value Pairs
  ▸ AVP: t=User-Name(1) l=7 val=hosuk
  ▸ AVP: t=Class(25) l=50 val=434143533a33444339413843303030303030303343343732...
  ▸ AVP: t=EAP-Message(79) l=6 Last Segment[1]
  ▸ AVP: t=Message-Authenticator(80) l=18 val=b183417c4d20dc138f59a29cee568ccf
  ▸ AVP: t=EAP-Key-Name(102) l=67 val=\031]AQ\264\034=5\213J&\323x\032\256\354\267c~\023&\t\360\344
  ▾ AVP: t=Vendor-Specific(26) l=67 vnd=ciscoSystems(9)
      Type: 26
      Length: 67
      Vendor ID: ciscoSystems (9)
    ▸ VSA: t=Cisco-AVPair(1) l=61 val=ACS:CiscoSecure-Defined-ACL=#ACSACL#-IP-Permit_All-5d41486b
  ▾ AVP: t=Vendor-Specific(26) l=38 vnd=ciscoSystems(9)
      Type: 26
      Length: 38
      Vendor ID: ciscoSystems (9)
    ▸ VSA: t=Cisco-AVPair(1) l=32 val=cts:security-group-tag=0004-00
  ▸ AVP: t=Vendor-Specific(26) l=58 vnd=Microsoft(311)
  ▸ AVP: t=Vendor-Specific(26) l=58 vnd=Microsoft(311)
```

Digital Certificates – Self-Signed



- Endpoint needs to validate server certificate prior to sending its credentials
- Identity certificate is also used to encrypt the communication

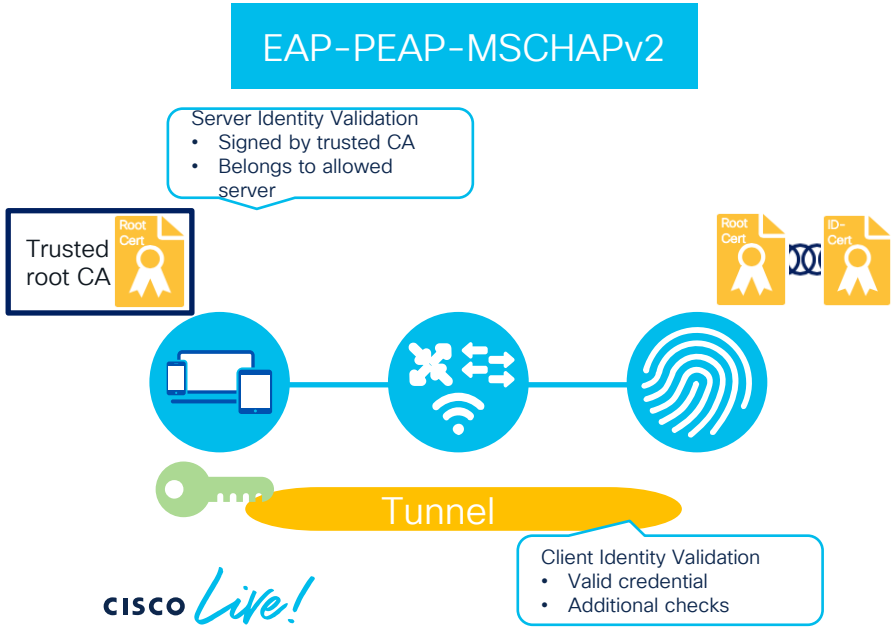
Digital Certificates – CA signed certificate validation

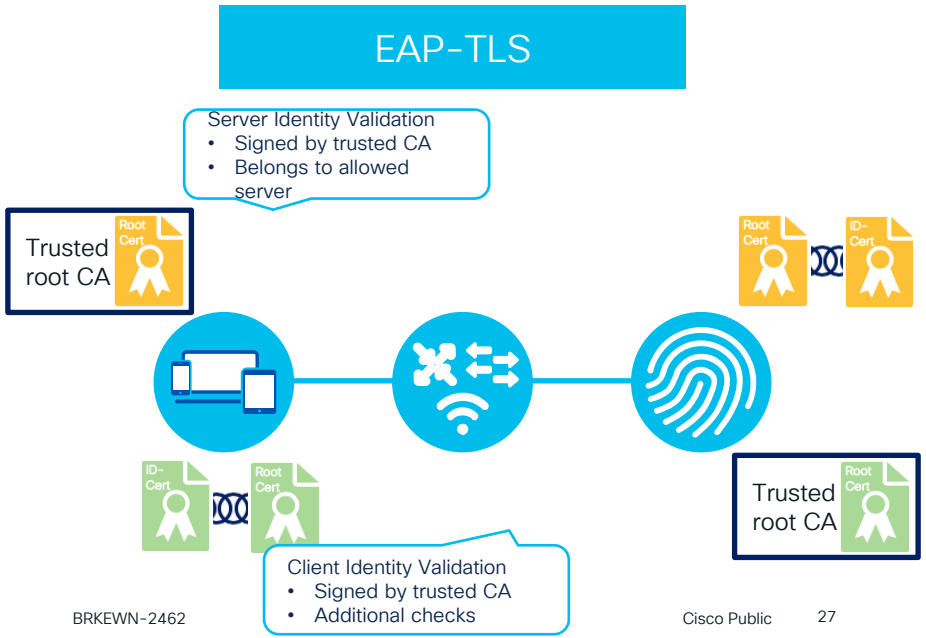


- Endpoint needs to validate server certificate prior to sending its credentials
- Identity certificate is also used to encrypt the communication

EAP-PEAP-MSCHAPv2 vs. EAP-TLS

- Both: Use of server certificate
- EAP-TLS: Mutual certificate authentication
- EAP-PEAP: Use of tunnel to encrypt transport





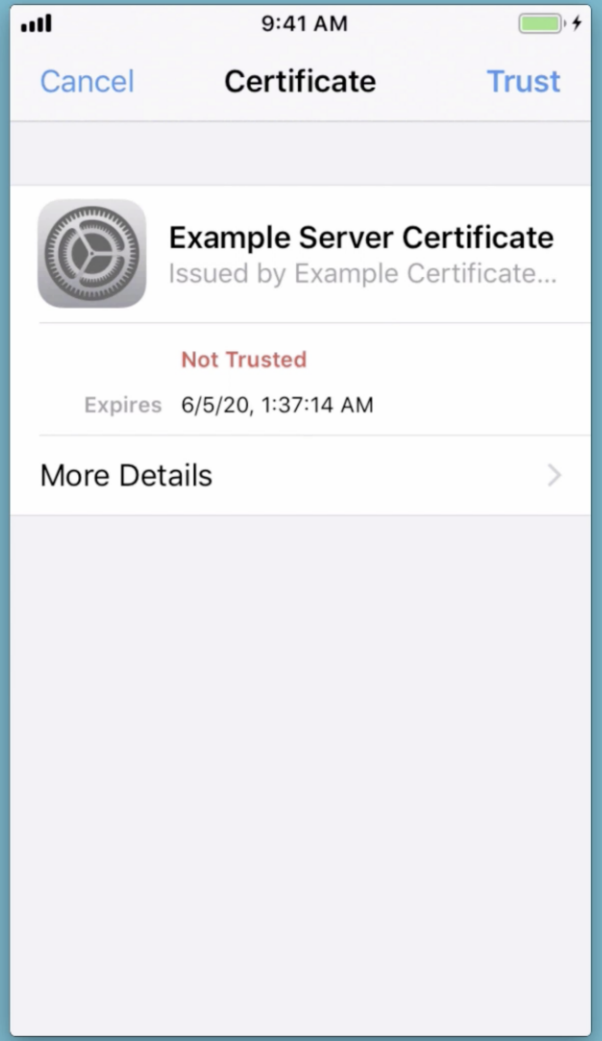
Certificate use on Browser vs. Supplicant

- User is aware of the destination
- Generally user is prompted before submitting credentials
- Browser compares destination host name to the certificate CN or SAN
- Optionally browser can check server certificate against CRL or OCSP

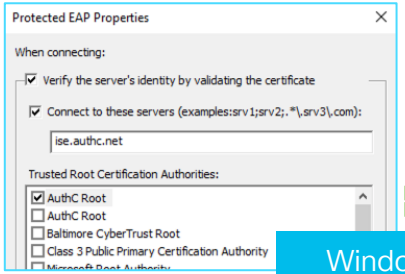
- Supplicant automatically connects using SSO or cached credentials
- Supplicant needs to be configured to trust specific CA (Does not trust O/S certificate store by default)
- Supplicant can be configured to check certain string in CN
- SSIDs can be brought up by anyone
- No network access during authentication to validate certificate via CRL or OCSP

howon — howon@kali-vm: ~ — ssh 192.168.201.235 — 113×45

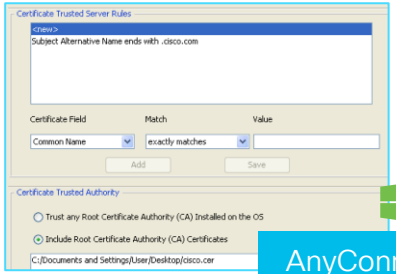
```
root@kali-vm:~#
root@kali-vm:~# hostapd-wpe /etc/hostapd-wpe/hostapd-wpe.conf
Configuration file: /etc/hostapd-wpe/hostapd-wpe.conf
Using interface wlan0mon with hwaddr 80:1f:02:68:62:d5 and ssid "@EMPLOYEE"
random: Only 16/20 bytes of strong random data available
random: Not enough entropy pool available for secure operations
WPA: Not enough entropy in random pool for secure operations - update keys later when the first station connects
wlan0mon: interface state UNINITIALIZED->ENABLED
wlan0mon: AP-ENABLED
wlan0mon: STA 08:e6:89:2d:26:4d IEEE 802.11: authenticated
wlan0mon: STA 08:e6:89:2d:26:4d IEEE 802.11: associated (aid 1)
wlan0mon: CTRL-EVENT-EAP-STARTED 08:e6:89:2d:26:4d
wlan0mon: CTRL-EVENT-EAP-PROPOSED-METHOD vendor=0 method=1
wlan0mon: CTRL-EVENT-EAP-PROPOSED-METHOD vendor=0 method=25
wlan0mon: STA 08:e6:89:2d:26:4d IEEE 802.1X: Identity received from STA: 'hosuk'
wlan0mon: STA 08:e6:89:2d:26:4d IEEE 802.1X: Identity received from STA: 'hosuk'
wlan0mon: CTRL-EVENT-EAP-RETRANSMIT 08:e6:89:2d:26:4d
```



Endpoint Supplicant Management & Configuration

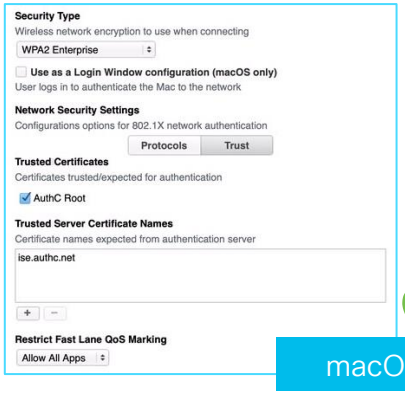


Windows GPO

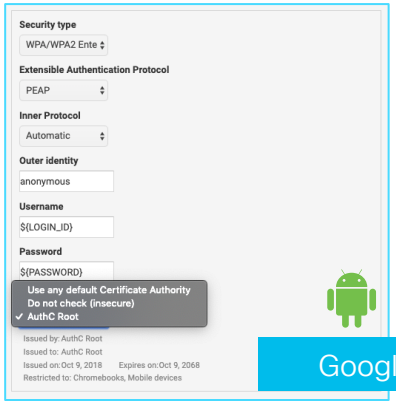


AnyConnect NAM

ISE BYOD



macOS Server



Google Suite

MDM/EMM

Cloud vs. On-prem identity

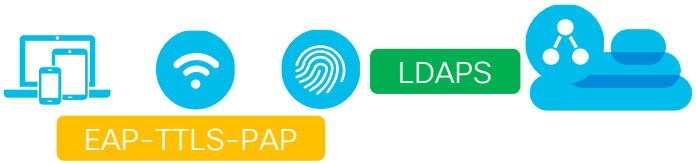
Cloud identity provider

On-prem identity provider

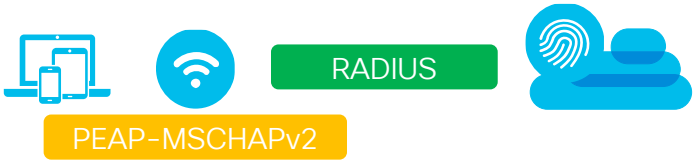
Protocols	SAMLv2, OpenID Connect	MSCHAPv2, PAP, MAC-Filtering
Requested access	Application, VPN	802.1X, Network access

OIDC – Open ID Connect

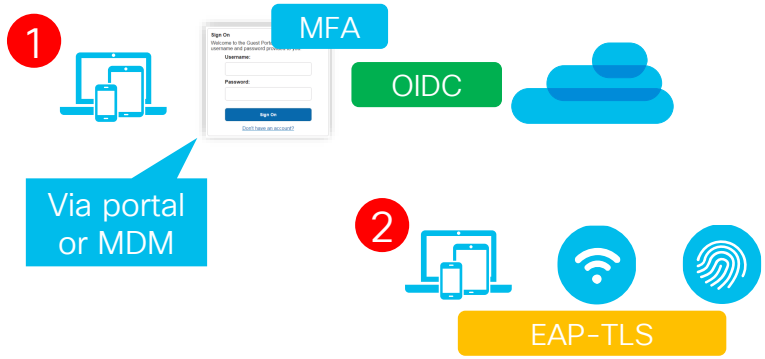
Utilize cloud identity for network access

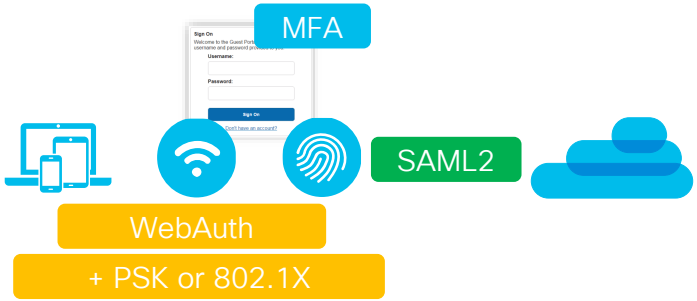


TTLS – Tunneled TLS



ROPC – Resource Owner Password Credentials



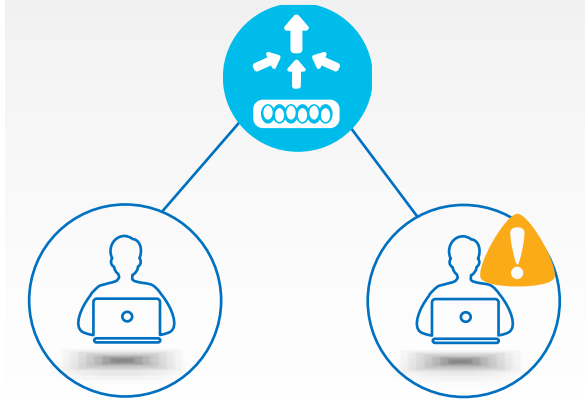


Access Control

Authorization Options

Named ACL

Named ACL

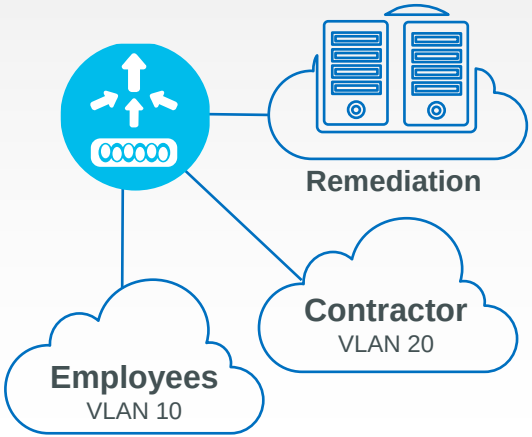


Healthy
permit ip any any

Non-compliant
permit ip host <remediation>
deny ip any any

VLANs

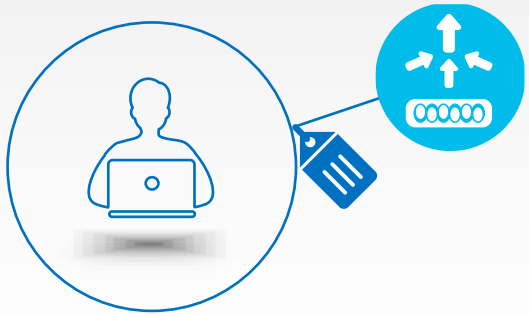
Dynamic VLAN Assignments



Per user / Per group / Per MAC

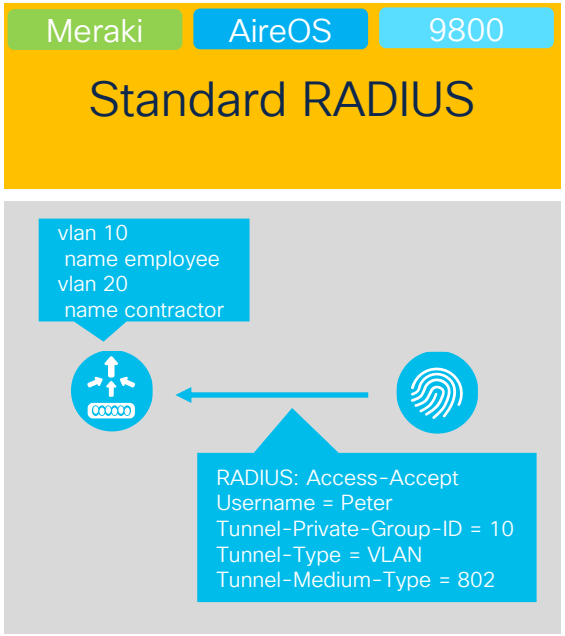
UDN ID or Tags

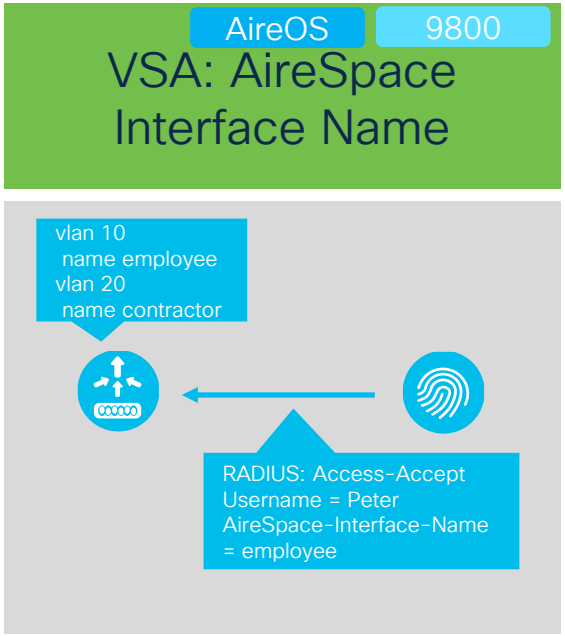
User Defined Network
or group tags

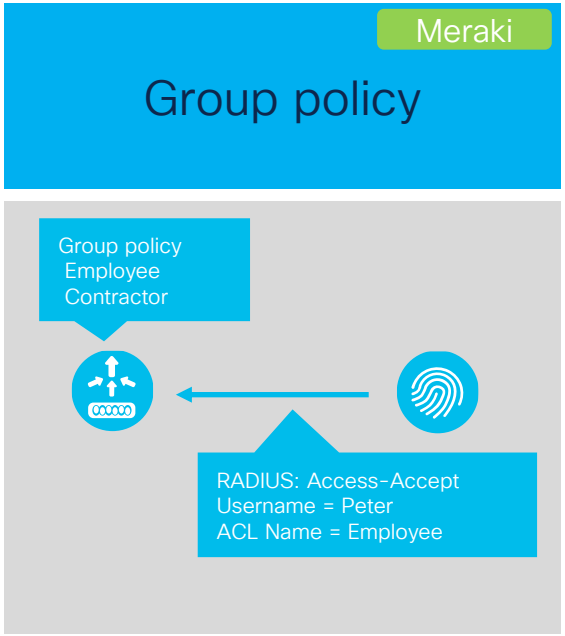


16 bit UDN ID Access Control for personal network or Security Group tags for group based policies

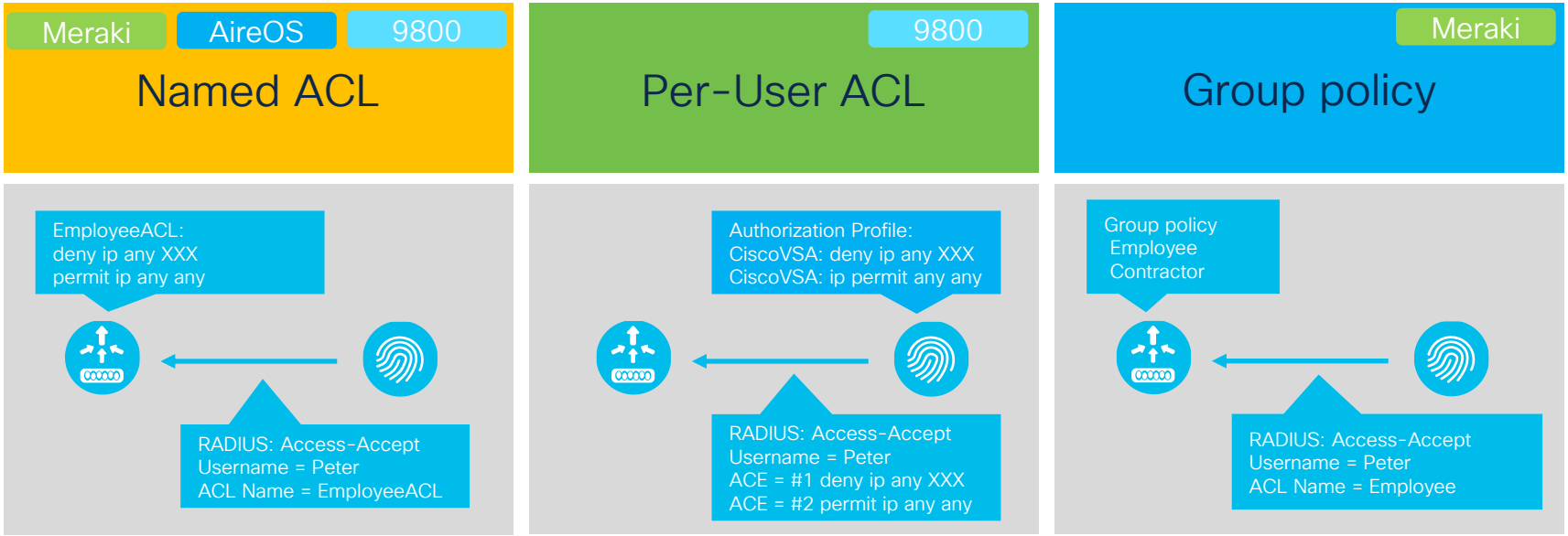
Dynamic VLAN





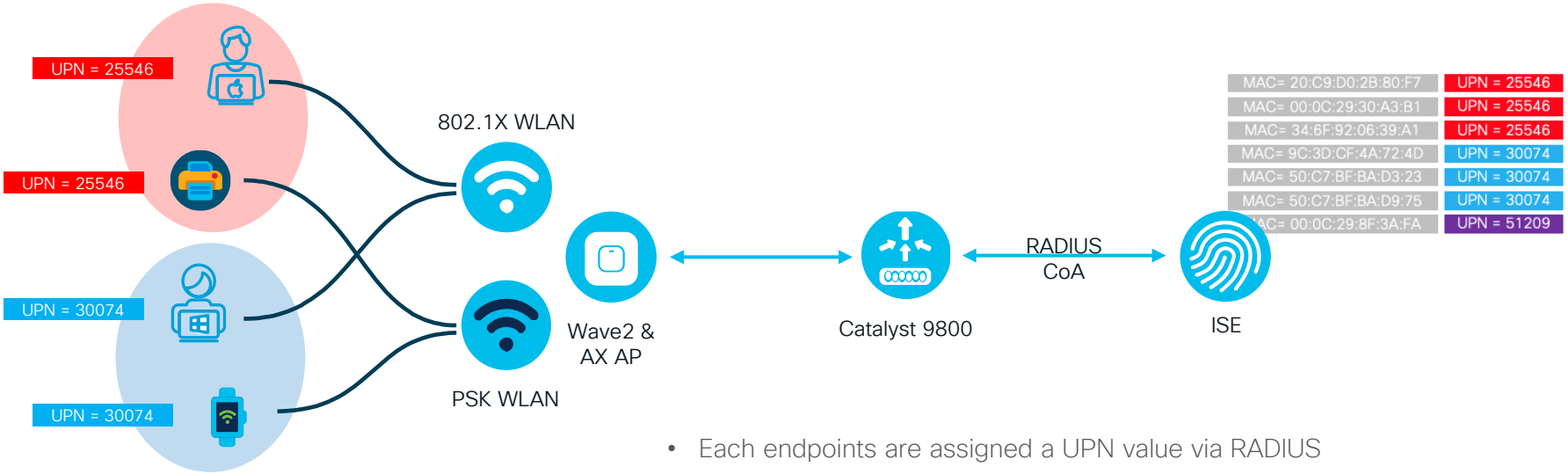


RADIUS enforced ACLs



Group tags (Meraki Adaptive policies)

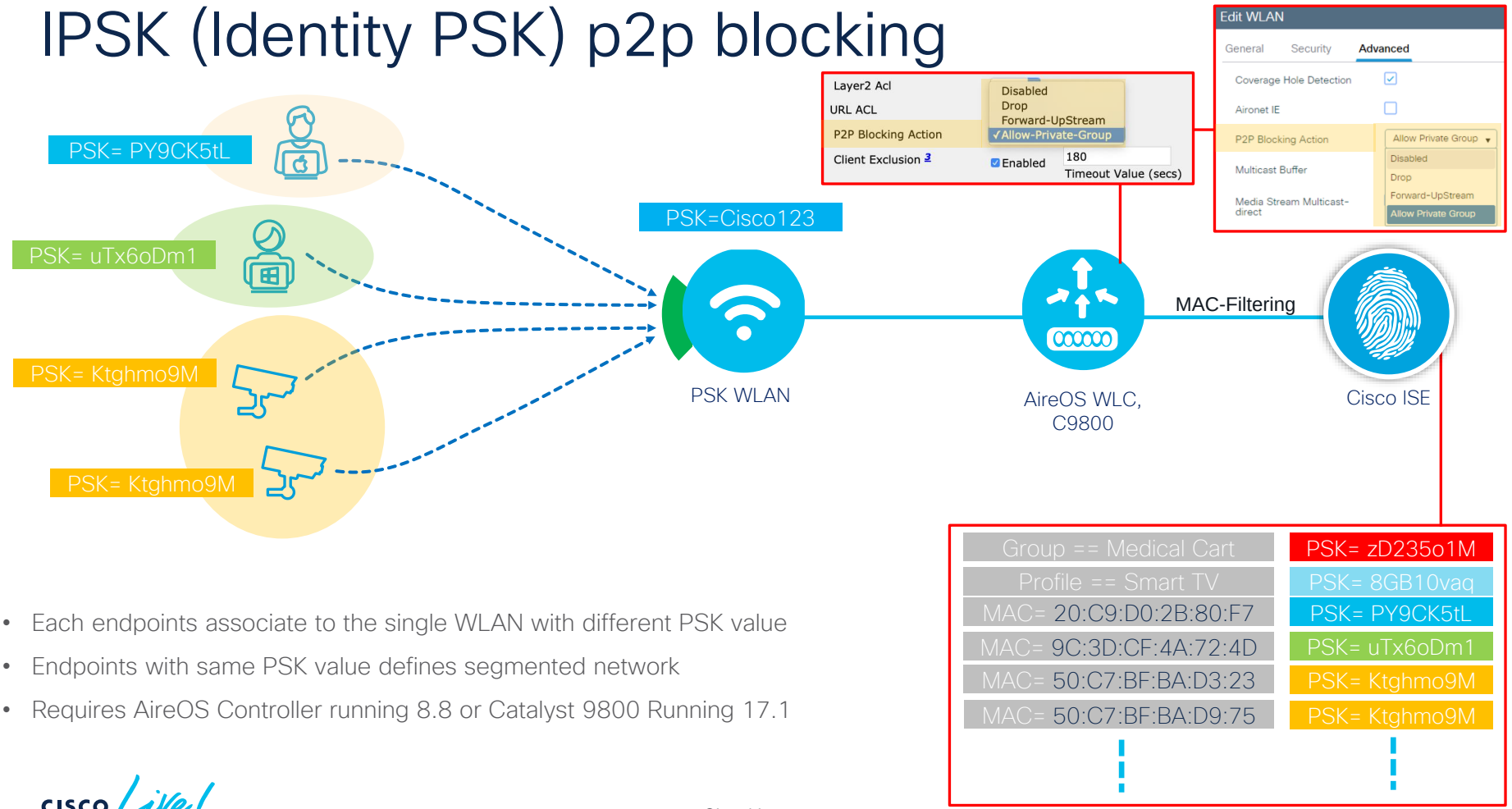
User Defined Network – Feature



- Each endpoints are 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

IPSK (Identity PSK) p2p blocking

AireOS | 9800



- Each endpoints associate to the single WLAN with different PSK value
- Endpoints with same PSK value defines segmented network
- Requires AireOS Controller running 8.8 or Catalyst 9800 Running 17.1

Additional 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

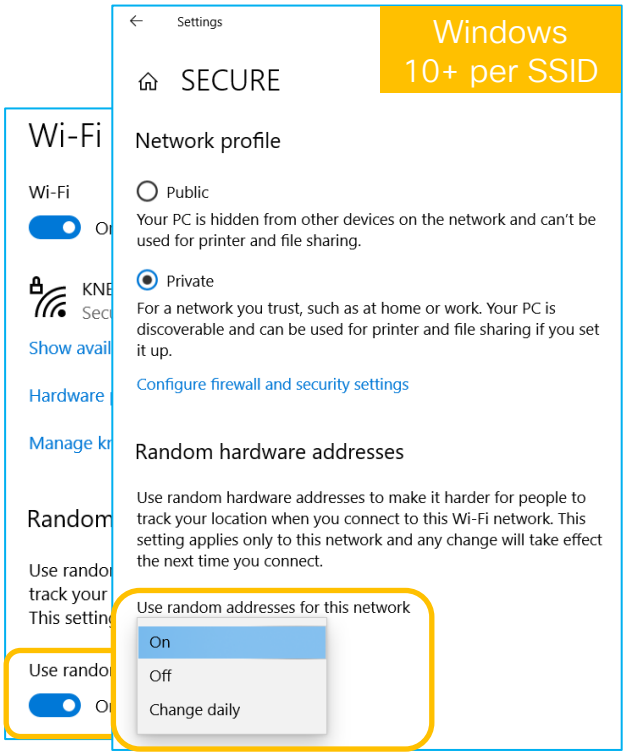
Assigns Open DNS profile to intercept DNS packets for custom response

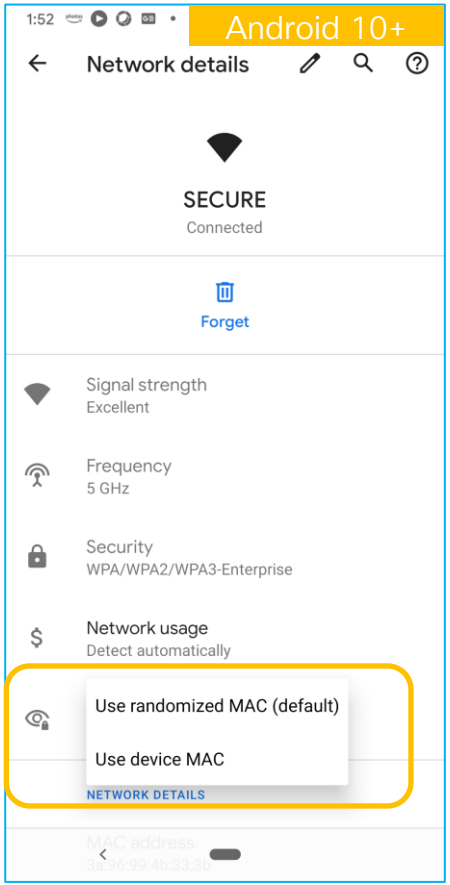
Service Template & Roles

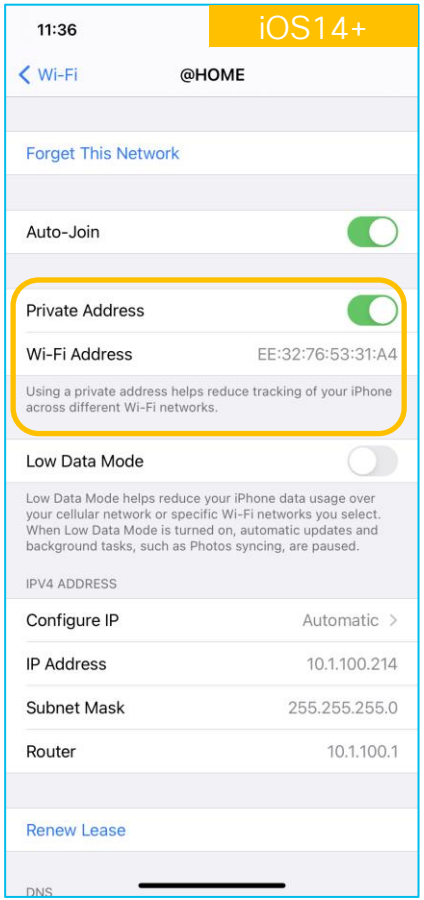
Assigns multiple access characteristics: VLAN, ACL, QoS, Timer, etc.

Quick note on the randomized MAC addresses

Implementation







Detailed implementation

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

Impact to network operations

Profiling

BYOD

Whitelisting

MDM Flow

Guest

Location lookup

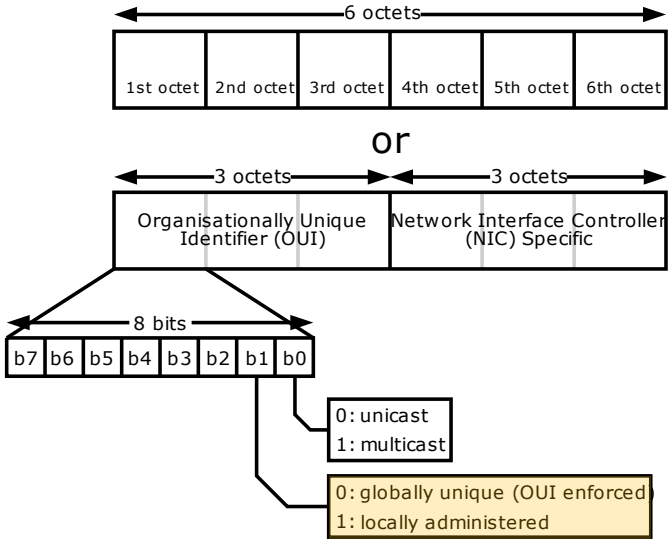
User Defined Network

Endpoint Analytics

Forensics

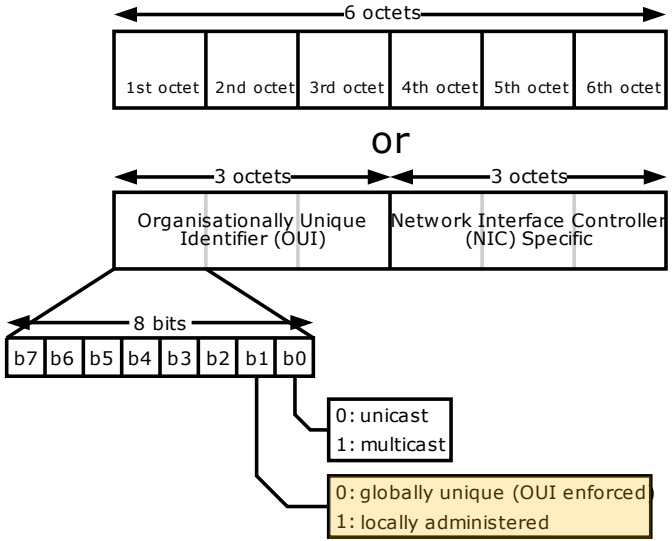
Quarantine

Can we detect it?



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

Can we detect it?



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

- 3**2**-28-6D-51-13-AF
- 5**6**-EF-68-F6-0D-30
- 0**A**-13-A8-8E-B5-EF
- A**E**-83-37-55-A7-22

02-	32-	62-	92-	C2-	F2-
06-	36-	66-	96-	C6-	F6-
0A-	3A-	6A-	9A-	CA-	FA-
0E-	3E-	6E-	9E-	CE-	FE-
12-	42-	72-	A2-	D2-	
16-	46-	76-	A6-	D6-	
1A-	4A-	7A-	AA-	DA-	
1E-	4E-	7E-	AE-	DE-	
22-	52-	82-	B2-	E2-	
26-	56-	86-	B6-	E6-	
2A-	5A-	8A-	BA-	EA-	
2E-	5E-	8E-	BE-	EE-	

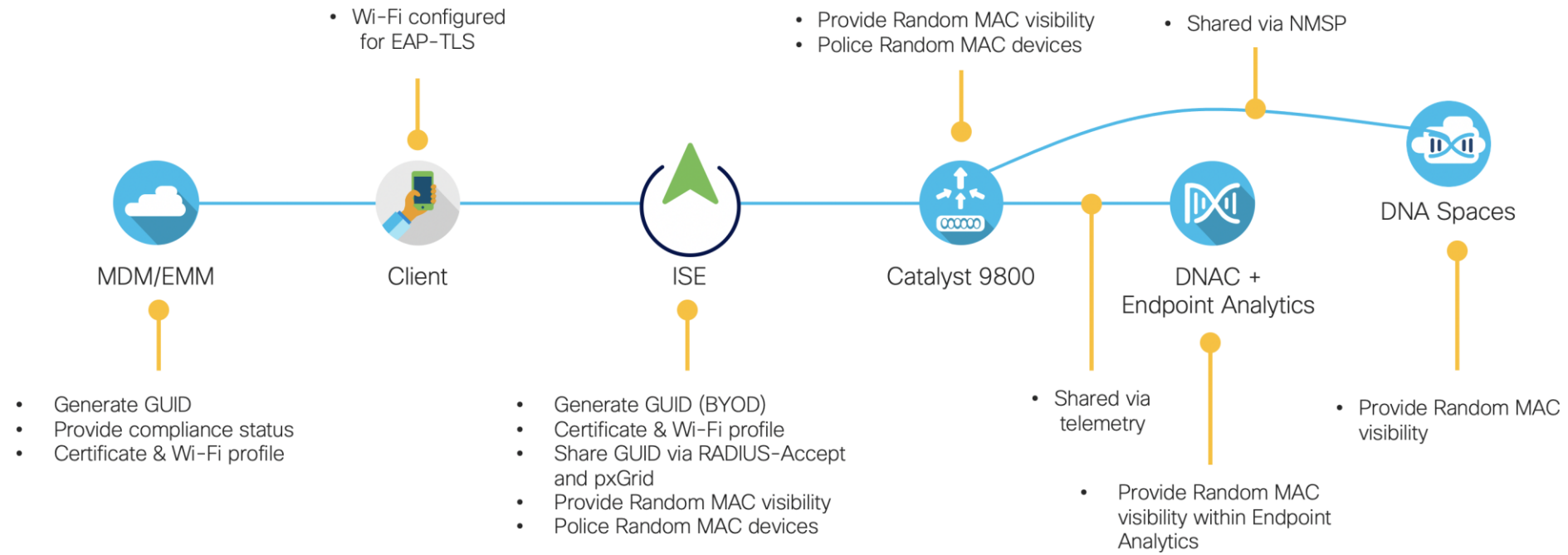
How can we use it?

```
▾ RADIUS Protocol
    Code: Access-Request (1)
    Packet identifier: 0x11 (17)
    Length: 339
    Authenticator: 0e65974db0ce6d4bd83ac3d8958eb096
    [The response to this request is in frame 2]
  ▾ Attribute Value Pairs
    ▸ AVP: t=User-Name(1) l=7 val=hosuk
    ▸ AVP: t=NAS-IP-Address(4) l=6 val=192.168.100.150
    ▸ AVP: t=NAS-Identifier(32) l=50 val=ce4f8c763ba3fe33b3c4af39a18fc4a687ddb4985cb7e421
    ▸ AVP: t=Called-Station-Id(30) l=26 val=62-3A-0E-FF-F9-82:SECURE
    ▸ AVP: t=NAS-Port-Type(61) l=6 val=Wireless-802.11(19)
    ▸ AVP: t=Service-Type(6) l=6 val=Framed(2)
    ▸ AVP: t=NAS-Port(5) l=6 val=1
    ▸ AVP: t=Calling-Station-Id(31) l=19 val=3A-96-99-4B-33-3B
    ▸ AVP: t=Connect-Info(77) l=56 val=CONNECT 54.00 Mbps / 802.11ac / RSSI: 54 / Channel: 44
    ▸ AVP: t=Acct-Session-Id(44) l=18 val=4CA46544377C0CF1
    ▸ AVP: t=Unknown-Attribute(186) l=6 val=000fac04
    ▸ AVP: t=Unknown-Attribute(187) l=6 val=000fac04
    ▸ AVP: t=Unknown-Attribute(188) l=6 val=000fac01
    ▸ AVP: t=Vendor-Specific(26) l=24 vnd=Meraki Networks, Inc.(29671)
    ▸ AVP: t=Vendor-Specific(26) l=8 vnd=Meraki Networks, Inc.(29671)
    ▸ AVP: t=Vendor-Specific(26) l=8 vnd=Meraki Networks, Inc.(29671)
    ▸ AVP: t=Vendor-Specific(26) l=25 vnd=Meraki Networks, Inc.(29671)
    ▸ AVP: t=Framed-MTU(12) l=6 val=1400
    ▸ AVP: t=EAP-Message(79) l=12 Last Segment[1]
    ▸ AVP: t=Message-Authenticator(80) l=18 val=0e2772128f681702f980afd95fbc67ec
```

Status	Rule Name	Conditions	Profiles	Security Groups
✓	Random MAC	Radius·Calling-Station-ID **MATCHES** ^.[26AEae].*	Select from list +	Select from list +

```
^.[26AEae].*
```

Addressing random MAC addresses



NMSP – Network Mobility Services Protocol

Call to action

- Move away from simple PSK
- 802.1X can be vulnerable – Deploy wireless profiles using MDM
- Understand pros/cons when utilizing cloud identity for network access
- Even with Zero Trust, secure with segmentation
- Random and Private MAC addresses can be managed

Technical Session Surveys

- Attendees who fill out a minimum of four session surveys and the overall event survey will get Cisco Live branded socks!
- Attendees will also earn 100 points in the Cisco Live Game for every survey completed.
- These points help you get on the leaderboard and increase your chances of winning daily and grand prizes.

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

Here at the event? Visit us at **The Learning and Certifications lounge at the World of Solutions**

Continue your education

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

cisco Live!

Thank you


cisco Live!
ALL IN